(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
25 May 2001 (25.05.2001)

PCT

(10) International Publication Number
WO 01/37546 A2

(51) International Patent Classification[7]: H04N 5/00, 7/167

(21) International Application Number: PCT/EP00/11483

(22) International Filing Date:
17 November 2000 (17.11.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/444,495 19 November 1999 (19.11.1999) US

(71) Applicant: SCM MICROSYSTEMS GMBH [DE/DE]; Sperl-Ring 4 Hettenshausen, 85276 Pfaffenhofen (DE).

(72) Inventors: VANTALON, Luc; 1396 Cordilleras Avenue, Sunnyvale, CA 94087 (US). CHATAIGNIER, Arnaud; 31, allée de la Granette, F-13600 Ceyreste (FR). GENEVOIS, Christophe; 47, avenue de la Paix, F-13600 La Ciotat (FR).

(74) Agent: DEGWERT, Hartmut; Prinz & Partner, Manzingerweg 7, 81241 München (DE).

(81) Designated States *(national)*: JP, SG.

(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Published:
— *Without international search report and to be republished upon receipt of that report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 01/37546 A2

(54) Title: DIGITAL TELEVISION METHODS AND APPARATUS

(57) Abstract: Conditional access methods and apparatus are provided for use with digital television receivers and other digital broadband receivers. The methods and apparatus are capable of handling several different digital signal transmission protocols in an automatic and flexible manner. An input unit is provided for analyzing and tagging incoming data bytes so that further processing operations are less dependent on the transmission format being received. A cipher handling unit is provided for adapting in real time the scrambling and descrambling performances to match the requirements of the transmission network and the receiving apparatus. A filtering mechanism is provided for filtering and handling multiple asynchronous data streams in a parallel manner.

DIGITAL TELEVISION METHODS AND APPARATUS

DESCRIPTION

CROSS-REFERENCE TO RELATED APPLICATIONS

This application is related to the following copending patent applications: U.S. Serial No. 09/444,488 , filed on Nov. 19, 1999 , entitled "Digital Television Conditional Access Methods and Apparatus with Multiple Data Transport Mechanism" and invented by Luc Vantalon, Arnaud Chataignier, and Christophe Genevois ; U.S. Serial No. 09/444,490 , filed on Nov. 19, 1999 , entitled "Adaptive Trans-Scrambling Mechanism for Digital Television Multiple Data Transport System" and invented by Luc Vantalon, Arnaud Chataignier, and Christophe Genevois; and U.S. Serial No. 09/443,173 , filed on Nov. 19, 1999 , entitled "Signal Filtering Mechanism for a Multi-Purpose Digital Television Receiver" and invented by Luc Vantalon, Arnaud Chataignier, and Christophe Genevois . The foregoing cross-referenced patent applications are expressly incorporated in their entirety into this application by this reference thereto.

TECHNICAL FIELD

This invention relates to digital television systems and services and particularly to conditional access methods and apparatus for use with such systems and services.

BACKGROUND OF THE INVENTION

Digital television is an emerging technology which is becoming increasingly popular with the public. One of the more interesting aspects is the introduction of so-called "high-definition television" (HDTV), the broadcasting of which was recently approved by the United States Federal Communications Commission. HDTV will provide television images of much higher quality and definition than is provided by preexisting "conventional definition" television systems.

Another highly important aspect of digital television is the providing of related services, such as video-on-demand programming, pay-per-view movies and sporting events, interactive video games, home shopping capabilities, high-speed Internet access and the like. The home television set is fast becoming the predominate information and services dispensing medium of the future.

As is known, television services are presently communicated by land-based radio-type broadcast transmissions, cable network transmissions and space satellite transmissions. In order to limit reception to paid subscribers, it is common practice for cable and satellite providers to scramble their transmissions and to require their customers to use a special set-top control box to unscramble the received signals. Such scrambling and set-top box techniques are also desired by providers of related services. The problem to date is that each provider has developed its own unique and proprietary set-top control box. Thus, to receive and use signals from multiple providers requires the use of multiple set-top control boxes. This is not the best

situation and, in order to overcome the problem, the U. S. Federal Communications Commission is encouraging a so-called "open" set-top box approach for providing a universal set-top box capable of receiving and handling content from multiple providers. Unfortunately, this is not an easy thing to do and at the same time provide the security control features needed to protect the various service providers from loss of services to unauthorized users.

SUMMARY OF THE INVENTION

The present invention provides an efficient and flexible adaptive receiving system for use in providing a "universal" set-top control box. This receiving system grants conditional access to the transmitted program material in a manner which provides a high degree of protection against unauthorized use of the material. This adaptive receiving system includes receiving circuitry for receiving signals from a network, such signals being in a selected one of a plurality of transport formats and in a selected one of a plurality of encryption formats. This system also includes circuitry for examining the received signals and generating transport format independent information signals relating thereto. This system further includes trans-scrambling circuitry for descrambling network encrypted portions of the received signals and rescrambling such portions in accordance with a copy protect encryption format required for the end user. Filtering circuitry is provided for extracting auxiliary information from the received signals and the system further includes control circuitry

responsive to the transport format independent information signals and to the extracted auxiliary information for controlling the trans-scrambling circuitry.

For a better understanding of the present invention, together with other and further advantages and features thereof, reference is made to the following description taken in connection with the accompanying drawings, the scope of the invention being pointed out in the appended claims.

BRIEF DESCRIPTION OF THE DRAWINGS

Referring to the drawings:

FIG. 1 is a general block diagram of a digital television receiving system with a security mechanism for preventing unauthorized display of the transmitted images;

FIGS. 2A-2D show different ways of packaging the apparatus of FIG. 1;

FIG. 3 is a conceptual diagram for one embodiment of the present invention;

FIG. 4 shows in greater detail a representative form of internal construction for the set-top box and the conditional access module of FIG. 2B;

FIG. 5 is a detailed block diagram for the transport stream co-processor and the microprocessor unit of the conditional access module of FIG. 4;

FIG. 6 shows a representative form of construction for an out-of-band channel feature of the present invention;

FIG. 7 shows a representative form of construction for a microprocessor-to-microprocessor data channel feature of the present invention;

FIG. 8 shows a representative form of construction for a Smart Card channel feature of the present invention;

FIG. 9 shows representative form of construction for the transport stream (TS) input unit of FIG. 5;

FIG. 10 shows in more detail a representative form of construction for the cipher bank unit of FIG. 5;

FIG. 11 shows a general form of construction for the cipher processor of FIG. 10;

FIG. 12 shows the details of a representative form of construction for the conditional access descrambler of FIG. 11;

FIG. 13 shows the details of a representative form of construction for the copy protect scrambler of FIG. 11;

FIG. 14 shows a representative form of construction for the filter bank unit of FIG. 5;

FIG. 15 shows in greater detail the construction of one of the filter units of FIG. 14;

FIG. 16 is a plan view of one form of PCMCIA Smart Card reader that may be used with the present invention;

FIG. 16A is a left end view of the FIG. 16 card reader;

FIG. 16B is a right end view of the FIG. 16 card reader;

FIG. 16C is a side view showing one side of the card reader of FIG. 16;

FIG. 17 is a perspective view of another form of PCMCIA card reader that may be used with the present invention;

FIG. 18 shows a further form of card reader that may be used;

FIGS. 19, 20 and 21 show the packet formats for different types of data transport streams that may be handled by the present invention;

FIG. 22 is a flow chart used in explaining a multiple data transport feature of the present invention;

FIG. 23 is a detailed flow chart for a representative implementation of the method of FIG. 22;

FIG. 24 shows another embodiment of the cipher bank unit of FIG. 5;

FIG. 25 is a timing diagram for an input stream interface according to the present invention; and

FIG. 26 is a timing diagram for an output stream interface according to the present invention.

DETAILED DESCRIPTION OF THE ILLUSTRATED EMBODIMENTS

Referring to FIG. 1, there is shown a general block diagram of a digital broadband receiving system having one or more receivers 10 connected to one or more broadband signal transmission networks. Typical signal transmission networks include land-based radio-frequency type broadcast networks, cable networks, space satellite signal transmission networks, broadband telephone networks, etc. The analog

information signals intended for transmission (for example: video signals, audio signals, or data signals) are converted to specific digital transport stream formats for transmission purposes. Typical transport stream formats are the MPEG format, the DSS format and the ATM format. The MPEG format is the data transmission format developed by the Motion Picture Expert Group. A preferred form of MPEG is MPEG-2, which is defined in ISO/IEC Standard 13818. The acronym "DSS" stands for Digital Satellite Systems and refers to a format developed for use in transmitting digital signals used by some satellite operators. The acronym "ATM" stands for Asynchronous Transfer Mode. It is a digital signal protocol for efficient transport of both fixed rate and bursty information in broadband digital networks. The ATM digital stream consists of fixed length packets called "cells."

Each receiver 10 demodulates its received signal and supplies the demodulated signal to a security mechanism 11. Security mechanism 11 selects one or more of the received signal transport streams and removes the network distribution security layers therefrom, provided the end user is entitled to receive the signals. Network security mechanism 11 also applies content protection to any of the signal streams that require it. The resulting signals are supplied to decoders 12 which select one or more of the signal streams and decodes each selected stream to recreate the desired video, audio and data signals which are, in turn, supplied to one or more display units 13 and one or more recording units 14. Typical display units include television sets and television and computer monitors. Typical recording units include VCR-type video recorders

and various types of computer memory units. Security mechanism 11 examines the received signal or signals and determines their types and controls their descrambling. Security mechanism 11 allows access to an unscrambled version of the received signal, provided the required conditions are met.

In addition to regular digital television programming, the receiving system of FIG. 1 also receives and handles various related communications services. Examples of related services are video-on-demand programming, pay-per-view movies and sporting events, interactive video games, home shopping services, high-speed Internet access, and the like. As will be seen, the data signals and control signals for these related services are supplied by way of a so-called "out-of-band" channel.

FIGS. 2A-2D show different ways of packaging the apparatus of FIG. 1. In particular, FIG. 2A shows the case where the receivers 10, security mechanism 11 and decoders 12 are located within a network specific set-top box 15. In one case, the security mechanism 11 is imbedded within or permanently mounted within the set-top box 15. In a typical use, the set-top box 15 sits on top of the display unit 13.

FIG. 2B shows an open-type set-top box 16 with a renewable and removable add-on security mechanism represented by a conditional access module (CAM) 17. Conditional access module 17 performs the security functions provided by the security mechanism 11 of FIG. 2A. Control access module 17 is a removable plug-in type element which is adapted to be plugged into a cooperating receptacle or socket in the host set-top box 16. As in FIG. 2A, set-top box 16 is designed to sit on top of the

display unit 13.

FIG. 2C shows the case where the set-top box functions are located inside the cabinet 18 of a television receiver, that is, the cabinet which houses the display unit or picture tube 13. The conditional access module 17 is adapted to plug into a cooperative receptacle which is accessible from the outside of the cabinet 18. FIG. 2C represents an integrated television set with a renewable, add-on security mechanism represented by the conditional access module 17.

FIG. 2D represents the case where the primary units are located in separate component-type cabinets or boxes 19a-19d. The conditional access module 17 may be removably plugged into the receiver box 19a or the decoder box 19b or may, instead, be part of a small connector unit which is connected between boxes 19a and 19b. The configuration of FIG. 2D would be particularly useful in a component-type entertainment center intended for home use.

Referring to FIG. 3, there is shown a conceptual diagram for one embodiment of the present invention. As there seen, the receiving apparatus includes an in-band channel 20 and an out-of-band channel 21, which are adapted to receive incoming signals from a remote broadcasting station. The in-band channel 20 handles the primary user signals, such as the digital television signals. The out-of-band channel 21, on the other hand, handles the digital signals for the related services, such as video-on-demand commands, security data, e-commerce transactions, etc. Both of channels 20 and 21 communicate with various application programs 22 by way of a

filter bank 23 which detects various defined digital patterns within the received signals and reacts thereto for establishing connections with the appropriate ones of applications 22.

The apparatus of FIG. 3 also includes a smart card channel 24 for providing communications between a smart card SC and the applications programs 22. A data channel 25 provides communications between a CPU (Central Processing Unit) located in the host unit, for example, set-top box (STB) 16, and the application programs 22. An extended channel 26 is provided to transfer network data over the out-of-band channel from the network to the host CPU or vice versa.

Referring to FIG. 4 there is shown in greater detail a representative form of internal instruction for the host unit or set-top box 16 and the conditional access module 17 of FIG. 2B. As seen in FIG. 4, a signal connector 29 connects the set-top box 16 to the communications network supplying the signals. This signal path 29 runs to an in-band receiver 30 and an out-of-band receiver 31. The communications network is a multi-channel system and the channel conveying the primary video and audio signals is labeled as the "in-band" channel and the channel which carries the signals for the related services is called the "out-of-band" channel. The set-top box 16 further includes an out-of-band transmitter 32 for transmitting signals back to the digital data provider located at the network broadcasting center.

The digital signals appearing at the outputs of receivers 30 and 31 are supplied to the conditional access module 17. The primary video and audio signals are

supplied back to a decoder 33 in the set-top box 16 and from there to the digital TV display 13. The set-top box 16 includes a microprocessor unit 34 which, among other things, provides control signals to the decoder 33. A memory unit 36 is coupled to the microprocessor unit 34 and, among other things, provides storage for various control routines and application program functions utilized by the microprocessor unit 34. Microprocessor unit 34 and memory 36 provide a CPU function for the set-top box 16.

The conditional access module (CAM) 17 of FIG. 4 includes a transport stream (TS) co-processor 40 which receives the output digital signals from the in-band receiver 30 and the out-of-band receiver 31, the latter being supplied by way of an out-of-band decoder 41. Transport stream co-processor 40 also supplies the digital video and digital audio signals which are intended for the TV display 13 to the decoder 33. Conditional access module 17 further includes a microprocessor unit 42 and an associated memory unit 43. These units 42 and 43 provide a CPU function for the conditional access module 17. The primary portion of the application programs 22 are stored in the memory 43. A data channel 44 provides a direct communications link between the CAM microprocessor unit 42 and the host microprocessor unit 34. The CAM microprocessor unit 42 can also send digital messages and information back to the network broadcasting center. This is done by way of an out-of-band encoder 45 and the out-of-band transmitter 32 in the host set-top box 16. A removable smart card 28 is adapted to be connected to the microprocessor unit 42 for supplying control information thereto.

An extended channel is provided for enabling the network broadcasting center to communicate with the host microprocessor unit 34 and vice-versa. The incoming branch of this extended channel includes a signal path 47 coupled to the out-of-band receiver 31 and extending to the out-of-band decoder 41. This incoming branch includes the decoder 41, transport stream co-processor 40, microprocessor 42 and a further signal path 49 which runs from the microprocessor 42 to the host microprocessor 34. The outgoing branch of this extended channel is provided by a signal path 50 which runs from the host microprocessor 34 directly to the out-of-band encoder 45.

Referring to FIG. 5, there is shown a detailed block diagram for the transport stream (TS) co-processor 40 and the microprocessor unit 42 of the conditional access module (CAM) 17 of FIG. 4. As seen in FIG. 5, the transport stream (TS) co-processor 40 includes a transport stream (TS) input unit 52 which receives parallel-type digital input signals TSin1 and TSin2 from the in-band receiver 30 and the out-of-band receiver 31, respectively. A serial-type digital signal TSin3 is received from the out-of-band receiver 31. The output signals from the input unit 52 are supplied to a cipher bank 54 for further processing. Cipher bank 54 produces two parallel type output streams which are connected to the inputs of a TS output unit 55 and a filter bank 56. By multiplexer selection within the cipher bank 54, one of the two input streams to the cipher bank 54 is processed by an internal cipher processor, while the other input stream is simply bypassed to the TS output unit 55 and the filter bank 56.

The TSout signal from TS output unit 55 is supplied to the decoder 33 in the set-top box 16 .

The transport stream input unit 52 includes a multiple data transport mechanism capable of receiving a plurality of different transport stream formats. In particular, it includes a qualifying mechanism for receiving and qualifying incoming data bytes according to their positions and values in their plural-byte data packets. TS input unit 52 further includes a tagging mechanism for assigning a plural-bit tag to each data byte, such tag having a unique value determined by the results of the qualifying process. The tag bits are used to facilitate the further processing of the data bytes.

The microprocessor unit 42 includes an ARM7 microprocessor 60 which is connected to a 32-bit ARM system bus ASB which typically operates in a high speed transfer mode. Also connected to the ASB bus are a memory interface unit 61, an address decoder unit 62, an arbiter unit 63, and a read only memory (ROM) unit 64. Memory interface 61 is connected to the external memory 43 associated with the microprocessor unit 42.

The microprocessor 60 communicates with the transport stream coprocessor 40 and various other units by means of a VLSI peripheral bus VPB. This VPB bus is connected to the microprocessor 60 by way of a bus-to-bus bridge unit 65 and the high- speed ASB bus. The ASB bus is used for fast transfers and the VPB bus is used for communications with a lower priority. As the filter bank 56 of co-processor 40

needs a direct and fast access to the external memory 43 for its ouput data, it is also connected to the ASB bus. As a consequence, there are three masters on the ABS bus, namely, the microprocessor 60 and the two channels of the filter bank 56. The arbitration between these masters is managed by the arbiter unit 63. By way of comparison, the VPB bus has only a single master, namely, the microprocessor 60.

The address decoder 62 decodes the address bits on the ASB bus to select the right target for the data on the ASB bus. Typical targets are the memory interface 61, ROM 64 and the various peripherals and other units connected to the ASB bus. An interrupt controller 66 provides the interrupt function for the microprocessor 60, while a timer 67 provides various timing functions. Each of the the units in the transport stream co-processor 40 is coupled to the lower priority VPB bus for control and status purposes. Also coupled to the VPB bus are an extended channel unit 68, a data channel unit 69 and a PCMCIA interface 70. A peripheral interface unit 71 provides an interface between the VPB bus and one or more peripheral devices. For example, a smart card interface connector structure 72 is provided for making connection with a removable smart card 28 shown in FIG. 4. A serial interface 73 may be provided for connecting to a serial type peripheral device PD.

FIG. 6 shows a representative form of construction for an out-of-band channel feature of the present invention. This out-of-band channel feature includes an out-of-band channel decoder 41 which receives the out-of-band signal OBin from the out-of-band receiver 31 shown in FIG. 4. The output of decoder 41 is supplied by way of the

transport stream co-processor 40 for further filtering operations. The outgoing or transmitter portion of the out-of-band channel includes ATM encoder 45, transmit buffer 46 and a channel encoder 48 which supplies the out-of-band output signal OBout to the out-of-band transmitter 32 shown in FIG. 4. The ATM encoder 45 receives its input signal from the VPB peripheral bus associated with the microprocessor unit 42. The data to be transmitted is supplied by either the application programs located in the microprocessor unit 42 or the data received from the set-top box 16 by way of the extended channel path 50. This data is segmented into ATM cells by the ATM encoder 45. These cells are temporarily stored in a buffer 46. When the network grants some transmission slots to the conditional access module 17, the transmit buffer 46 is emptied by channel encoder 48 and is transmitted by way of out-of-band transmitter 32 to the network broadcast center.

FIG. 7 shows a microprocessor-to-microprocessor data channel feature of the present invention. This feature enables the CAM microprocessor unit 42 to communicate directly with the host microprocessor unit 34 and vice-versa. Microprocessor unit 42 sends data to the microprocessor unit 34 by way of data channel 44a. The host unit 34 sends data to the CAM microprocessor 42 by way of data channel 44b.

FIG. 8 shows the details of the smart card interface 72 of FIG. 5. The smart card 28 is adapted to be inserted into a smart card reader 86 and the data received from the smart card 28 is supplied by way of an input buffer 87 to the peripheral bus VPB

associated with the microprocessor unit 42. Data from the microprocessor unit 42 is supplied by way of the VPB bus, output buffer 88 and the smart card reader 86 to the smart card 28. In a representative embodiment, smart card reader 86 is a PCMCIA card reader. The acronym PCMCIA stands for Personal Computer Memory Card International Association. This is a non-profit trade association founded in 1989 to define a standard memory card interface. The smart card reader 86 complies with this interface standard.

Referring now to FIG. 9 there is shown in greater detail a representative form of construction for the transport stream input unit 52 of FIG. 5. The TSin1 and TSin2 signals are supplied to input registers 130 and 131. The serial input signal TSin3 is supplied to a serial-to-parallel converter 132 which converts same from serial form to parallel form. The parallel output of converter 132 is supplied to a further input register 133. The outputs of registers 130, 131, and 133 are connected to a three-to-two multiplexer 134. This multiplexer 134 selects two out of the three inputs and supplies one of the selected inputs to a TS1 FIFO unit 135 and the other of the selected inputs to a TS2 counter unit 136. FIFO 135 provides the input for a TS1 parser 137, while the counter 136 provides the input for a TS2 parser 138. Parsers 137 and 138 analyze their respective signal streams on a byte-by-byte basis and assign a plural-bit tag to each data byte. More particularly, each of parsers 137 and 138 includes a qualifying mechanism for receiving and qualifying incoming data bytes according to their positions and values in their plural-byte data packets. In a

representative embodiment, a 5-bit tag is generated for and attached to each data byte. The value of this 5-bit tag is determined by the qualifying process performed by the qualifying mechanism. Parsers 137 and 138 are, in turn, connected to a selection parser 139 which determines the particular output path, TSa or TSb, to which each data stream is connected.

Referring to FIG. 10, there is shown in more detail a representative form of construction for the cipher bank 54 of FIG. 5. Cipher bank 54 receives the two signal streams TSa and TSb from the TS input unit 52 of FIG. 9. The two output buses 74 and 75 from cipher bank 54 are connected to the TS output unit 55 and the filter bank 56. Thus, the cipher bank 54 has two input streams and two output streams. By selection via multiplexers 76, 77, and 78, one of the input streams is processed by a cipher processor 79, while the other input stream is simply bypassed to the output of its corresponding one of multiplexers 77 and 78. Multiplexers 76, 77 and 78 are controlled by selection signals S1, S2 and S3, respectively, obtained by way of the VPB bus.

For a first set of multiplexer settings, the TSa data stream is transferred by way of multiplexer 76 to the cipher processor 79 and the output of cipher processor 79 is transferred by way of multiplexer 77 to the TSout1 bus 74 of the cipher bank 54. For this same case, the second input data stream TSb, is supplied by way of multiplexer 78 to the TSout2 bus 75. For the second set of multiplexer settings, the situation is reversed. The TSb data stream is supplied by way of multiplexer 76 to the cipher

processor 79 and the resulting processed signal is supplied by way of multiplexer 78 to the TSout2 bus 75. In this second case, the TSa input data stream is supplied by way of multiplexer 77 to the TSout1 bus 74. Cipher processor 79 outputs both a protected data stream TSp and a clear data stream TSc. Multiplexers 77 and 78 select one or the other, but not both of these data streams.

Referring to FIG. 11, there is shown the primary elements of the cipher processor 79 of FIG. 10. As seen in FIG. 11, cipher processor 79 includes a conditional access descrambler 80 and a copy protection scrambler 81. Descrambler 80 descrambles a scrambled incoming digital signal to produce a clear copy output signal TSclear. Descrambler 80 is capable of descrambling the following encryption formats: the DVB super scrambling format used in Europe, the DES and 3DES data encryption standard formats which are used in the United States, and the MULTI2 format which is used in Japan. The copy protect scrambler 81 is used to rescramble the clear copy signal at the output of descrambler 80 to preclude the data content from being stolen at the output of the conditional access module 17. Scrambler 81 uses the DES data encryption standard scrambling method.

FIG. 12 shows the details of a representative form of construction for the conditional access descrambler 80 of FIG. 11. The descrambler 80 of FIG. 12 includes an input data register 140 for receiving the TSin data stream from the multiplexer 76 of FIG. 10. Descrambler 80 also includes a set of eight decoders 141-148 for descrambling any one of the following encryption formats: DVB, DES-ECB,

DES-CBC, DES-OFB, MULTI2, 3DES-ECB, 3DES-CBC and 3DES-OFB. Other encryption formats can be accommodated by providing appropriate additional decoders. The foregoing acronyms have the following meanings:

ACRONYM	DESCRIPTION
DVB	Digital Video Broadcasting (Europe)
DES	Data Encryption Standard (U.S.)
ECB	Electronic Code Book
CBC	Chain Block Cipher
OFB	Ouput Feedback Block

The ECB, CBC and OFB formats are known variations of the DES and 3DES formats.

A descramble format register 150 and an associated decoder 151 determine which one of the primary decoders 141-148 is activated to process the incoming data stream. Descramble format register 150 is loaded by way of the VPB bus with a plural-bit control signal which designates the decoder to be used. This control signal is decoded by the enable signal decoder 151 to activate one and only one of its output lines. Thus, only a selected one of the decoders 141-148 is activated or used for any given data transport stream.

It is also necessary to load a session key register 152 with a descrambling session key which tells the selected one of decoders 141-148 how to descramble the incoming data stream. This descrambling key is loaded into register 152 by way of the VPB bus. Register 152, in turn, supplies the descrambling key to each of the

decoders 141-148 and it is used by the decoder which is selected by the control signal in the descramble format register 150. The descrambled data stream appearing at the output of the selected one of decoders 141-148 is supplied to an output data register 153 to provide a clear or unscrambled output signal TSclear or TSc.

Referring now to FIG. 13, there is shown the details of a representative form of construction for the copy protect scrambler 81 of FIG. 11. For the embodiment shown in FIG. 13, the descrambler 81 includes a set of three encoders 155, 156 and 157 for encoding the TSclear signal from descrambler 80 in accordance with any one of the following three encryption formats: DES-ECB, DES-CBC and DES-OFB. Other scrambling formats may be used if desired. Selection of a desired one of the encoders 155-157 is accomplished by means of a plural-bit 7 control signal which is loaded into a scramble format register 158. This control signal controls an enable signal decoder 159 to activate a select one of its output lines, which output lines individually run to different ones of the encoders 155-157. The scrambled data stream appearing at the output of the selected encoder is supplied to an output data register 160 to provide the copy protected output signal TSprotected or TSp. The actual scrambling process which is followed in the selected encoder is controlled by a plural-bit scrambling session key which is loaded into a session key register 161. This scrambling session key is obtained from the microprocessor unit 42 by way of the VPB bus.

Referring now to FIG. 14, there is shown a representative form of construction for the filter bank 56 of FIG. 5. This filter bank 56 examines incoming data streams to

determine the type of data packets being received. When a desired packet is identified, its data payload is then stored in the proper location in memory 43 which is assigned to its particular packet type. In this way, the incoming data may be filtered or sorted according to the application or use for which it is intended. More particularly, the filter bank 56 has two inputs FLTin1 and FLTin2 which may convey different transport stream formats. For example, the first input FLTin1 can be connected to the in-band channel output from in-band receiver 30 and its data stream is assumed to use the MPEG packet format. The second input FLTin2 can receive the data stream from the out-of-band receiver 31 and the data signals of the this out-of-band channel are assumed to be of the asynchronous transfer mode (ATM) cell format.

The filter bank 56 includes four filter units 90-93 which can be independently set up to process different data streams. This architecture allows a flexible adjustment of the filtering resource depending on the type of application. For example, if the conditional access module is set up to support ATSC-type advanced television services (for example, high-definition television), the four filter units 90-93 are tuned to the in-band channel. For an open cable type of operation, on the other hand, up to three of the filter units can be set to process the out-of-band channel for collecting IP and proprietary messages, while the fourth filter unit must stay tuned to the in-band channel for processing in-band command signals. The outputs of filter units 90-93 are selectively connected to the microprocessor ASB bus by a multiplexer 94 which is controlled by switching signal S4.

FIG. 15 shows in greater detail a representative form of construction for one of the filter units 90-93 of FIG. 11. Each of the filter units 90-93 is of this same construction. The filter unit of FIG. 12 is tuned to one of the two inputs FLTin1 and FLTin2 by a multiplexer 95 which is set to select one of the two inputs by a selector signal S5. The selected input data stream is supplied to a Type Filter 96 which prefilters the data bytes according to the plural-bit tags attached to them in the TS input unit 52 of FIG. 9. The filtered bytes are then stored in an array of filter cells 97a-97h. Pre-recorded signal pattern which it is desired to detect are stored in a pattern memory 98 and are supplied to filter cells 97a-97h. When a pattern match occurs, the corresponding filter cell loads a shift register 99. Complete messages are extracted from shift register 99 for storage in the memory unit 43 associated with the CAM microprocessor unit 42.

FIG. 16 is a plan view of one form of PCMCIA smart card reader that may be used with the present invention. FIG. 16A is a left-end view, FIG. 16B is a right-end view and FIG. 16C is a side view of the card reader shown in FIG. 16. The acronym PCMCIA stands for Personal Computer Memory Card International Association. This is a non-profit trade association formed in 1989 to define a standard memory card interface. The smart card reader of FIG. 16 includes a metallic casing 100 which is adapted to receive a plastic memory card or smart card of approximately the size of a plastic credit card. The casing 100 conforms to ISO Standard 7816. In use, the smart card is inserted into the casing 100 and the casing 100 is, in turn, inserted into an

appropriate connector receptacle in the set-top-box 16.

FIG. 17 is a perspective view of another form of PCMCIA card reader that may be used with the present invention. The reader casing 101 of FIG. 17 has a shorter extension, hence, a shorter overall length. FIG. 18 shows a further form of card reader that may be used. The reader casing 102 of FIG. 18 is a so-called dual reader casing and is adapted to receive two different smart cards.

FIGS. 19, 20 and 21 show the packet formats for different types of data transport streams that may be handled by the present invention. FIG. 19 shows the format for an MPEG data stream packet. FIG. 20 shows the format for a DSS data stream packet and FIG. 21 shows the format for an ATM data stream cell. The MPEG format is the data transmission format developed by the Motion Picture Expert Group. The preferred form of MPEG is MPEG-2 which is defined in ISO/IEC Standard 13818. The acronym "DSS" stands for Digital Satellite Systems and refers to a format developed for use in transmitting digital signals by some satellite operators. The acronym "ATM" stands for Asynchronous Transfer Mode. It is a digital signal protocol for efficient transport of both constant rate and bursty information in broadband digital networks. The ATM digital stream consists of fixed-length packets called "cells". Each cell contains 53 8-bit bytes and is comprised of a 5-byte header and a 48-byte information payload. The digital television signal standard approved for use in the United States employs the MPEG-2 transport stream format for packeting and multiplexing the video, audio and data signals.

An MPEG packet has an overall length of 188 bytes and includes a 4-byte header field and a variable length adaptation field which can vary in length from zero bytes to several bytes. The remainder of the packet is comprised of payload bytes. A DSS packet has an overall length of 130 bytes and includes a 3-byte header field and an optional variable length adaptation field of relatively-small length. The remainder of the DSS packet is comprised of payload bytes.

FIG. 22 is a flow chart which explains the general nature of the multiple data transport feature of the present invention. Each newly received data byte (block 103) is examined and qualified according to its position and value in its data packet (block 125). The examined byte is then tagged with a plural-bit tag (block 126), the value of the tag being determined by the results of the qualifying process (block 125). The resulting tagged byte is then passed on as a qualified byte (block 124). In the present embodiment, the process described by FIG. 22 is performed by the TS input unit 52 shown in FIG. 9. The qualification and tagging of the received data bytes is performed by the parsers 137 and 138.

Referring to FIG. 23, there is shown a detailed flow chart for a representative implementation of the method of FIG. 22. This multiple transport method of FIG. 23 enables the conditional access module 17 to handle any of the MPEG, ATM and DSS transport stream formats. Each incoming data byte is qualified according to its position and value within its packet. This qualification mechanism attaches a 5-bit tag to each data byte, which tag contains all the information required for further

processing of the byte. The qualification of each new byte starts with block 103 of FIG. 23, which block represents the reception of the new byte. The byte is first examined to determine if it is a header byte (block 104). If it is, a determination is then made as to whether it contains channel identification (ID) data (block 105). If the answer is yes, the byte is assigned a 3-bit tag portion having a value of "011" (block 106). If it is not a channel ID, then the byte is assigned a 3-bit tag portion having a value of "010" (block 107). Note that the total tag is a 5-bit tag. The purpose of the other two bits will be described shortly.

If the determination of block 104 determines that the new byte is not a header byte, then the byte undergoes a series of further non-header byte tests. The first test, represented by block 108, is to determine whether the byte is a null byte. If yes, it is assigned a 3-bit tag having a code of "000", as indicated by block 109. If the answer is no, then the byte proceeds to an adaptation field test represented by block 110. If the byte is an adaptation field byte, then it is assigned a tag value of "101", as represented by block 111. If it is not an adaptation field byte, then the test of block 112 is performed to determine whether or not it is a table identification (ID) byte. If yes, the byte is assigned a 3-bit tag having a value of "110", as represented by block 113. If no, the byte is examined per block 114 to determined whether it is a section length indicator byte. If yes, it is assigned a 3-bit tag value of "001", as indicated at block 115. If no, the byte proceeds to the payload decision block 116. Since this is the only alternative left, the byte is determined to be a payload byte and is given a 3-

bit tag portion having a value of "111", as indicated at block 117.

After assignment of the initial 3-bit portion of its tag, the newly received byte is tested as indicated by decision block 118, to determine whether its data is scrambled or clear. If scrambled, a fourth bit in the tag, namely, the SCR bit is set to 1. If not scrambled, the SCR bit is set to 0. The byte is then tested as indicated by block 121 to determine whether it is the last byte of either a header field or a payload field. If it is a last byte, the LTB bit (the fifth bit in the 5-bit tag) is set to 1 (block 122) and if not, the LTB bit is set to 0 (block 123). This completes the qualification process and the qualified output byte at step 124 is now in condition for further processing in the conditional access module 17.

The qualification process of FIG. 23 produces a stream of output bytes which are no longer dependent on the particular transport stream format which brought them to the conditional access module 17. Thus, the conditional access module 17 is enabled to process a variety of different transport stream formats in an efficient manner with minimal complication. And while the described implementation supports the MPEG, DSS and ATM transport stream formats, it can be readily extended to handle other packet-type or cell-type transport structures.

FIG. 24 shows another embodiment of the cipher bank unit of FIG. 5.

FIG. 25 is a timing diagram for an input stream interface according to the present invention.

FIG. 26 is a timing diagram for an output stream interface according to the

present invention.

While there have been described what are at present considered to be preferred embodiments of this invention, it will be obvious to those skilled in the art that various changes and modifications may be made therein without departing from the invention and it is, therefore, intended to cover all such changes and modifications coming within the true spirit and scope of the invention.

CLAIMS

What is claimed is:

1. An adaptive receiving system comprising:

receiving circuitry for receiving signals from a network, such signals being in a selected one of a plurality of transport formats and in a selected one of a plurality of encryption formats;

circuitry for examining the received signals and generating transport format independent information signals relating thereto;

trans-scrambling circuitry for descrambling network encrypted portions of the received signals and rescrambling such portions in accordance with a copy protect encryption format required for the end user;

filtering circuitry for extracting auxiliary information from the received signals;

and control circuitry responsive to the transport format independent information signals and to the extracted auxiliary information for controlling the trans-scrambling circuitry.

2. An adaptive signal receiving method comprising:

receiving signals from a network, such signals being in a selected one of a plurality of transport formats and in a selected one of a plurality of encryption

formats;

examining the received signals and generating transport format independent information signals relating thereto;

descrambling network encrypted portions of the received signals and rescrambling such portions in accordance with a copy protect encryption format required for the end user;

extracting auxiliary information from the received signals;

and using the transport format independent information signals and the extracted auxiliary information for controlling the descrambling and rescrambling operations.

3. A method comprising:

receiving data in predetermined data units;

qualifying the received data units;

determining an encryption state of the data unit;

in the case of unencrypted data, providing a clear output; and

in the case of encrypted data, performing a decrypting function in accordance with the unit size.

4. The method according to claim 3 further comprising determining whether it contains identification data.

5. The method according to claim 4 including performing an adaptation test.

6. The method according to claim 5 including determining whether a payload byte is present.

7. The method according to claim 6 including determining whether the data is scrambled.

8. A system for handling a plurality of transport stream formats, said system comprising:

a qualification mechanism; and

a tagging mechanism for applying a multibit tag to each received data byte.

9. The system according to claim 8 including a mechanism for determining byte type.

10. The system according to claim 9 further comprising a mechanism for determining whether the byte contains a channel identifier.

11. The system according to claim 10, including performing an adaptation test.

12. The system according to claim 11 including a mechanism for identifying payload bytes.

13. The system according to claim 12 including a mechanism for determining whether the data received is scrambled.

14. The system according to claim 8 including a mechanism producing a stream of output bytes independent of the stream format in which they were received.

15. The system according to claim 8 configured to receive input transport streams formatted according to selected stream formats.

16. The system according to claim 8 configured to receive selected type transport structures.

17. A mechanism for receiving different transport stream formats, comprising:

a mechanism for qualifying incoming data bytes; and

a mechanism for assigning a tag to each incoming data byte.

18. A method comprising:

qualifying received data bytes according to character; and

attaching a tag to each received data byte.

19. A system comprising:

a plurality of receivers configured for communication with one or more signal transmission sources producing signals in a selected transport stream format; and

a security mechanism configured to select one or more of the received signal transport streams and to remove at least a single security layer therefrom.

20. The system according to claim 19, including a mechanism for content protection.

21. The system according to claim 19 further including a plurality of decoders.

22. The system according to claim 19 configured to examine received signals to determine their types.

23. The system according to claim 22 configured to control descrambling of received signals.

24. A system comprising:

a plurality of receivers configured for communication with one or more signal transmission sources subject to at least a single predetermined security layer; and

a mechanism configured to remove the at least a single security layer.

25. The system according to claim 23 wherein said mechanism is a conditional access module.

26. The system according to claim 23 including a display unit.

27. The system according to claim 23 configured to plug into a cooperative receptacle.

28. A system comprising:

a plurality of receivers configured in a selected transport stream format; and

a security mechanism configured to select one or more transport streams.

29. The system according to claim 28 wherein each of said plurality of receivers includes an in-band channel and an out-of-band channel.

30. The system according to claim 29 wherein said in-band and out-of-band channels are connected with a filter bank.

31. The system according to claim 28 further including a smart card channel.

32. The system according to claim 29 further configured to enable communications with at least a single application.

33. A system comprising:

an input signal channel for receiving a digital data stream in one of a plurality of different digital transmission formats;

circuitry for converting the incoming data stream into a transmission format independent set of signals;

and a display mechanism for converting the transmission format.

34. A system in accordance with claim 33 wherein:

the circuitry includes a qualifying mechanism for incoming data bytes;

and a tagging mechanism for assigning a tag to each data byte;

and the receiving system includes circuitry responsive to the tagged data bytes.

35. A system in accordance with claim 34 wherein the qualifying mechanism comprises a parser mechanism.

36. A system comprising:

at least two input channels for receiving at least two data streams, wherein each data stream is transmitted in one of a plurality of different formats;

circuitry for converting each incoming data stream into a format independent set of signals;

a mechanism for converting the format independent signals into an image;

and a message processing mechanism for converting the format independent message signals into perceivable messages.

37. A system in accordance with claim 36 wherein the circuitry comprises:

a first qualifying mechanism;

a first tagging mechanism;

first signal processing circuitry;

a second qualifying mechanism;

a second tagging mechanism;

and second signal processing circuitry responsive to the tagged message signal bytes for supplying message signals to the message processing mechanism.

38. A system in accordance with claim 37 wherein each qualifying mechanism comprises a parser mechanism.

39. A system comprising:

a qualifying mechanism;

a tagging mechanism;

and a signal processing mechanism responsive to tagged data bytes.

40. A mechanism comprising:

a qualifying mechanism;

and a tagging mechanism for assigning a plural-bit tag to each data byte.

41. A mechanism in accordance with claim 40 wherein the qualifying mechanism comprises a parser mechanism.

42. A mechanism comprising:

a first testing mechanism;

a first tagging mechanism coupled to the first testing mechanism for assigning header byte indicative tags;

a second testing mechanism for examining each incoming data byte and determining whether the data is scrambled;

a second tagging mechanism coupled to the second testing mechanism for assigning a scramble condition tag bit to each data byte and giving such bit one binary value if the data is scrambled and the other binary value if the data is not scrambled;

and signal transfer circuitry for transferring each data byte and its assigned tag bits to a data processing mechanism for producing usable digital information.

43. A method comprising:

receiving data in data units;

determining an encryption state of the data;

in the case of unencrypted data, providing a clear output; and

in the case of encrypted data, determining a unit size of the received data unit and performing a decrypting function in accordance with the unit size determined, thereby providing decrypted data.

44. The method according to claim 43, comprising:

selecting a desired scrambling format;

selecting a session key; and

loading a selected session key in a selected memory.

45. The method according to claim 43, comprising selecting a scrambling format.

46. The method according to claim 43, including processing broadcast signals.

47. The method according to claim 43, including processing burst signals.

48. A method of scrambling, comprising:

pairing a selected host with a selected module;

selecting a desired scrambling format; and

selecting a session key.

49. The method according to claim 48, comprising selecting a scrambling format from a group including DES-ECB, DES-CBC, and DES-OFB.

50. The method according to claim 49, including processing broadcast signals.

51. The method according to claim 49, including processing burst signals.

52. A method of descrambling, comprising:

pairing a selected host with a selected module;

selecting a desired descrambling format; and

selecting a session key.

53. The method according to claim 52, comprising selecting a descrambling format from a group including DVB, DES-ECB, DES-CBC, DES-OFB, MULTI2, 3DES-

ECB, 3DES-CBC and 3DES-OFB, wherein DVB means digital video broadcasting, DES means Data Encryption Standard, ECB means electronic code book, CBC means chain block cipher, and OFB means output feedback block.

54. The method according to claim 52, including processing broadcast signals for descrambling.

55. The method according to claim 52, including processing burst signals for descrambling.

56. The method according to claim 52 including descrambling with an input data register for receiving an TSin data stream.

57. The method according to claim 52 including using a descrambler having a plurality of decoders for descrambling any one of the following encryption formats: DVB, DES-ECB, DES-CBC, DES-OFB, MULTI2, 3DES-ECB, 3DES-CBC and 3DES-OFB, wherein DVB means digital video broadcasting, DES means Data Encryption Standard, ECB means electronic code book, CBC means chain block cipher, and OFB means output feedback block.

58. The method according to claim 52 including using a descramble format register

and an associated decoder to select which one of the plurality of decoders to activate for processing incoming data.

59. The method according to claim 52 including using a descramble format register.

60. The method according to claim 52 wherein said control signal is decoded by an enable signal decoder.

61. The method according to claim 60 including loading a session key register with a descrambling session key.

62. The method according to claim 60 including loading a descrambling key.

63. The method according to claim 60 including supplying a descrambling key.

64. The method according to claim 63 including selecting a decoder; and producing a descrambled data stream.

65. A scrambler comprising:

a scramble format register; and

a plurality of encoders configured to be individually selected by a control signal.

66. The scrambler according to claim 65 including an enable signal decoder.

67. The scrambler according to claim 65 configured to produce a scrambled data stream.

68. The scrambler according to claim 65 wherein scrambling is controlled by a scrambling session key.

69. The scrambler according to claim 65 wherein the scrambling session key is obtained from a microprocessor.

70. A method of scrambling comprising:

making a channel change;

selecting a descrambling mechanism;

making a session key change; and

loading a new session key.

71. A method of multiple scrambling according to claim 70, comprising:

receiving a qualified packet cell byte; and

determining whether the received qualified packet cell is scrambled, and if the received qualified packet cell is not scrambled, then outputting a clear packet cell byte.

72. A method comprising:

receiving a qualified packet cell byte; and

determining whether the received qualified packet cell is scrambled, and if the received qualified packet cell is not scrambled, then outputting a clear packet cell byte.

73. A method according to claim 72, wherein if the received qualified packet cell is scrambled, then a determination of full block status is made.

74. A method according to claim 73, wherein if the full block determination is negative, a reduced size block determination is made.

75. A method according to claim 72, comprising:

determining a copy protection status; and

if the copy protection status determination is negative, outputting a clear information.

76. A method of according to claim 72, comprising:

if the copy protection determination is affirmative, then a determination of block status is made; and

operation is undertaken according to the block status.

77. A method according to claim 72, wherein if the block determination for a first size is negative, a shorter block determination is made; and

if the shorter block determination is affirmative, then the shorter block operation is undertaken.

78. A method comprising:

receiving a qualified byte of data;

determining whether the received qualified byte is scrambled; and

if the received qualified byte is not scrambled, then clear information is output.

79. A method according to claim 78, wherein a determination is made with respect to copy protection; and

if the determination is negative, then producing clear information.

80. A method comprising:

qualifying received data bytes within a packet;

attaching a tag to each received data byte;

selecting a desired scrambling format; and

selecting a session key.

81. The method according to claim 80 further comprising examining each byte to determine its type.

82. The method according to claim 80 further comprising determining whether the byte contains a channel identification.

83. The method according to claim 80, including performing an adaptation field test.

84. The method according to claim 80, including determining whether the byte is a payload byte.

85. The method according to claim 80 including determining whether the data in the byte is scrambled.

86. The method according to claim 80 including producing a stream of output byte independent of particular transport stream format in which received.

87. A system comprising:

a qualification mechanism for processing received data bytes according to position and value;

a tagging mechanism for applying a tag to each received data byte;

a scramble format register; and

a plurality of encoders configured to be individually selected by a plural-bit control signal loaded into the scramble format register.

88. The system according to claim 87 including:

an enable signal decoder; and

a mechanism configured to produce a scrambled data stream at the output of a selected encoder.

89. The system according to claim 87 wherein scrambling is controlled by a plural-bit scrambling session key.

90. The system according to claim 87 wherein the scrambling session key is obtained from a microprocessor.

91. The system according to claim 87 including a mechanism for examining each received byte.

92. The system according to claim 87 further comprising a mechanism for determining whether the byte contains channel identification data.

93. The system according to claim 87, including a mechanism for performing an adaptation test.

94. The system according to claim 87 including a mechanism for determining whether the byte is a payload byte.

95. The system according to claim 87 including a mechanism for determining whether the data in the byte is scrambled.

96. The system according to claim 87 including a mechanism producing a stream of output bytes which are not dependent on a particular transport stream format.

97. The system according to claim 87 configured to receive input transport streams formatted according to selected transport stream formats.

98. The system according to claim 87 configured to receive selected transport structures.

99. A method for handling any of a plurality of signal formats, said method comprising:

qualifying received data bytes; and

attaching a tag to each received data byte to indicate whether a qualified data byte is scrambled and whether it is to be copy protected.

100. A system comprising:

a qualifying mechanism;

a tagging mechanism for assigning a tag to each data byte; and

a scramble format mechanism.

101. A system comprising:

a plurality of receivers configured for communication with one or more signal transmission sources producing signals in a selected signal format; and

a security mechanism configured to select a received signal stream for removal of a security layer depending upon block type.

102. The system according to claim 101, wherein said security mechanism applies content protection to predetermined signal streams.

103. The system according to claim 101 further including a plurality of decoders which are configured to select one or more of the signal streams.

104. The system according to claim 101 wherein said security mechanism is configured to type received signals.

105. The system according to claim 101 wherein said security mechanism is configured to control descrambling operation.

106. A system comprising:

a plurality of receivers configured for reception of a secure stream; and

a security mechanism configured to remove the network distribution security layers therefrom, according to block type.

107. A system according to claim 106 wherein said security mechanism is a removable element.

108. The system according to claim 106 wherein said security mechanism is adapted

to plug into a cooperative receptacle.

109. A system comprising:

a plurality of receivers configured for communication with a selected transport stream format; and

a security mechanism configured to select one or more of the received signal transport streams and to remove the network distribution security restrictions therefrom.

110. The system according to claim 109 wherein each of said plurality of receivers includes an in-band channel and an out-of-band channel.

111. The system according to claim 109 wherein said in-band and out-of-band channels are connected with a filter bank.

112. The system according to claim 109 further including a smart card channel.

113. A system comprising:

input circuitry for receiving a digital data signal which is scrambled according to different formats;

a mechanism for identifying the encryption format of the received signal;

a descrambling mechanism for descrambling the received data signal; and

a scrambling mechanism for rescrambling the descrambled data signal.

114. The system in accordance with claim 113 including a digital television receiving system.

115. A system in accordance with claim 113 including a television display mechanism for producing visual images.

116. A system in accordance with claim 113 including a video tape recorder.

117. A system in accordance with claim 113 wherein the received data signal is scrambled in accordance with a first data encryption format and rescrambled in accordance with a second data encryption format.

118. A system in accordance with claim 117 wherein the first data encryption format is a selected one of a DVB, DES-ECB, DES-CBC, DES-OFB, MULTI2, 3DES-ECB, 3DES-CBC and 3DES-OFB, wherein DVB means digital video broadcasting, DES means Data Encryption Standard, ECB means electronic code book, CBC means chain block cipher, and OFB means output feedback block format and the second data encryption format is a DES format.

119. A system in accordance with claim 118 wherein the scrambling mechanism produces a scrambled data signal which is different from the encryption format of the received signal.

120. A system in accordance with claim 118 wherein the received data signal is scrambled in accordance with a particular one of a first plurality of different data encryption formats, producing a scrambled data signal which is scrambled in accordance with a particular one of a second plurality of different data encryption formats.

121. A system in accordance with claim 118 wherein the scrambling sequence for the received data signal is controlled by a scrambling key.

122. A system in accordance with claim 118 wherein the descrambling mechanism comprises a plurality of decoder mechanisms for descrambling data signals and a decoder selection mechanism.

123. A system in accordance with claim 118 including a plurality of encoder mechanisms for scrambling in accordance with different data encryption formats and an encoder selection mechanism for selecting the particular encoder mechanism for scrambling clear information.

124. A method comprising:

decrypting information encrypted with a first type of encryption; and

re-encrypting said information with a second type of encryption.

125. A method comprising:

receiving qualified information;

determining the qualified information is scrambled; and

if not scrambled, passing the unscrambled information without scrambling it.

126. A method comprising:

selecting a channel for receiving information;

selecting a descrambling mechanisms; and

determining a descrambling session key to enable descrambling.

127. The method according to claim 126 including descrambling according to a determined mechanism and key.

128. The method according to claim 127 including rescrambling with a selected scrambling mechanism.

129. A method comprising:

pairing a selected conditional access module or card with a selected module;

selecting a copy protect mechanism; and

determining a scrambling session key.

130. A mechanism comprising:

circuitry for receiving multiple format transport streams;

a mechanism for identifying data bytes according to their position within their packet or cell;

a mechanism for identifying data bytes according to their value within their packet or cell and producing a match indication signal when a match is detected;

and a data extraction mechanism responsive to the match indication signal.

131. A mechanism in accordance with claim 130 including a pattern memory unit for identifying different user applications.

132. A mechanism in accordance with claim 130 including a plurality filtering cells

units for going after multiple section in parallel.

133. A mechanism in accordance with claim 130 including a mechanism for deactivating some filtering cells for increasing the specific section length of the active ones.

134. A mechanism in accordance with claim 130 including a shift register for extracting the data byte that have matched the specific section prior to their relevant payload.

135. A system comprising:

a detector for detecting different predefined digital patterns within received digital signals;

and circuitry for transferring data bytes associated with each of the different predefined digital patterns to different end use locations.

136. A system in accordance with claim 135 wherein the end use locations are different application programs.

137. A system comprising:

a plurality of filter units for receiving a plurality of digital data transport

streams and separating transport stream segments intended for different end uses;

a plurality of short term storage units for receiving the separated segments;

a long term storage unit;

and a multiplexer mechanism for coupling the short term storage units to the long term storage unit in a time shared manner.

138. A method comprising:

scrambling signals in accordance with a private cipher key before they are recorded;

and descrambling recorded signals in accordance with this same private cipher key when they are played back.

139. A method comprising:

receiving signals to be protected;

scrambling the received signals in accordance with a locally-generated cipher key;

recording the scrambled signals on a signal storage medium;

playing back the recorded signals;

descrambling the played-back signals in accordance with the locally-generated cipher key;

and supplying the descrambled signals to an end-user system.

140. A method comprising:

receiving signals to be protected;

scrambling the received signals in accordance with a locally-generated cipher key;

and recording the scrambled signals on a signal storage medium.

141. A method comprising:

playing recorded signals;

descrambling the played signals in accordance with a cipher key which is the same as a predetermined cipher key;

and supplying the descrambled signals to an end-user system.

142. A system comprising:

a scrambler mechanism responsive to a signal to be recorded for producing a scrambled version thereof which is scrambled in accordance with a predetermined key;

a recording mechanism for recording the scrambled signal on a storage medium to produce a protected copy thereof;

a playback mechanism for playing back scrambled signals recorded on the storage medium;

a descrambler mechanism responsive to played signals for descrambling such signals in accordance with the predetermined key;

and circuitry for supplying the descrambled signals to an end-user.

143. A system in accordance with claim 142 wherein the signals are digital signals.

144. A system in accordance with 142 wherein the signals are digital television signals.

145. A system in accordance with claim 142 wherein the signals are digital video signals.

146. A system in accordance with claim 143 wherein the signals are digital audio signals.

147. A system in accordance with claim 143 wherein the storage medium is a removable memory device.

148. A system in accordance with claim 142 wherein the storage medium is a computer storage medium.

149. A system in accordance with claim 142 wherein the storage medium is a magnetic medium.

150. A system in accordance with claim 142 wherein the signal storage medium is an optical storage medium.

151. A system in accordance with claim 142 wherein the signal storage medium is an integrated circuit memory device.

152. A system comprising:

a scrambler mechanism responsive to a signal to be recorded for producing a scrambled version thereof which is scrambled in accordance with a predetermined cipher key;

and a recording mechanism for recording the scrambled signal on a signal storage medium to produce a security protected recorded copy thereof.

153. A system comprising:

a playback mechanism for playing back scrambled signals recorded on a signal storage medium;

a descrambler mechanism responsive to the played back signals for descrambling such signals in accordance with the predetermined cipher key;

and circuitry for supplying the descrambled signals to an end-user system.

154. A system comprising:

a descrambler mechanism responsive to the received scrambled signals for descrambling same to produce a clear copy version thereof;

a scrambler mechanism responsive to the clear copy signals for scrambling such signals in accordance with a private cipher key;

and circuitry for supplying the privately-scrambled signals to a signal storage medium for producing a private recorded copy thereof.

155. A system in accordance with claim 154 wherein the descrambler mechanism descrambles the received signals in accordance with a transmitted cipher key.

156. A system in accordance with claim 154 wherein the transmitted cipher key is the same conditional access cipher key used by the conditional access system.

157. A system comprising:

a playback mechanism for playing back privately scrambled signals recorded on a signal storage medium, such privately scrambled signals having been scrambled in accordance with a private cipher key;

a descrambler mechanism for descrambling same in accordance with the

private cipher key to produce a clear copy version thereof;

a scrambler mechanism responsive to the clear copy signals for scrambling such signals in accordance with a copy protection cipher key used by the conditional access system;

and circuitry for supplying the cδpy protection scrambled signals to an end-user system.

158. A multiformat signal system comprising:

a multitransport system for receiving data;

a multiscrambling system for processing said received data; and

a multifiltering system for filtering said received data according to end-user application to separate user content from control data.

159. A method for processing control and content information having one of a plurality of formats and subject to scrambling, comprising:

receiving, qualifying and tagging according to qualification status, the received control and content information;

using the qualification tag to determined descrambling operation; and

separating the control from the content information.

160. An adaptive receiving system comprising:

receiving circuitry for receiving signals from a network, such signals being in a selected one of a plurality of encryption formats;

trans-scrambling circuitry for descrambling network encrypted portions of the received signals and rescrambling such portions in accordance with a copy protect encryption format required for the end user;

filtering circuitry for extracting auxiliary information from the received signals;

and control circuitry responsive to the extracted auxiliary information for controlling the trans-scrambling circuitry.

161. An adaptive receiving system comprising:

receiving circuitry for receiving signals from a network, such signals being in a selected one of a plurality of transport formats and in a selected one of a plurality of encryption formats;

circuitry for examining the received signals and generating transport format independent information signals relating thereto;

trans-scrambling circuitry for descrambling network encrypted portions of the received signals and rescrambling such portions in accordance with a copy protect encryption format required for the end user;

and control circuitry responsive to the transport format independent information signals for controlling the trans-scrambling circuitry.

162. An adaptive receiving system comprising:

receiving circuitry for receiving signals from a network, such signals being in a selected one of a plurality of transport formats and in a selected one of a plurality of encryption formats;

circuitry for examining the received signals and generating transport format independent information signals relating thereto;

trans-scrambling circuitry for descrambling network encrypted portions of the received signals and rescrambling such portions in accordance with a copy protect encryption format required for the end user;

and filtering circuitry for extracting auxiliary information from the received signals.

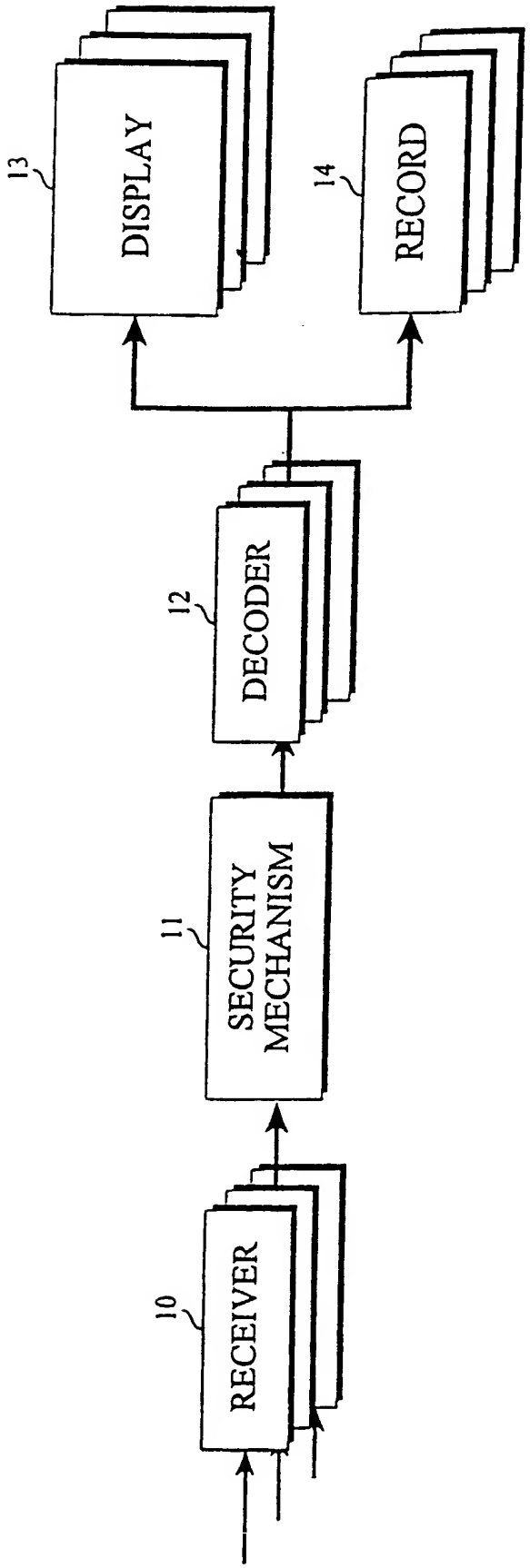

Fig. 1

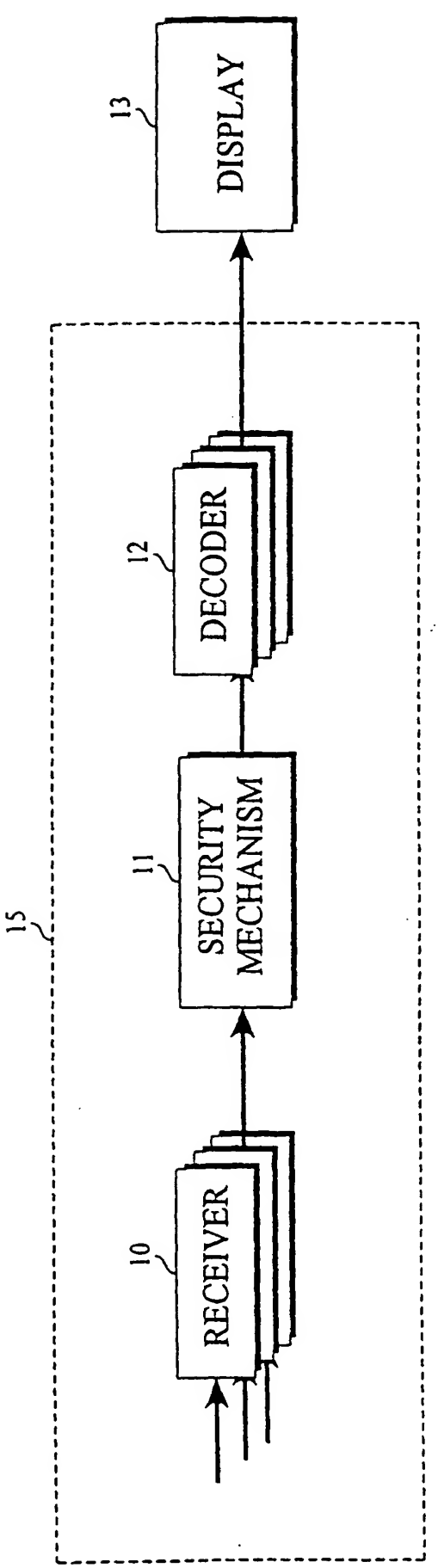

Fig. 2A

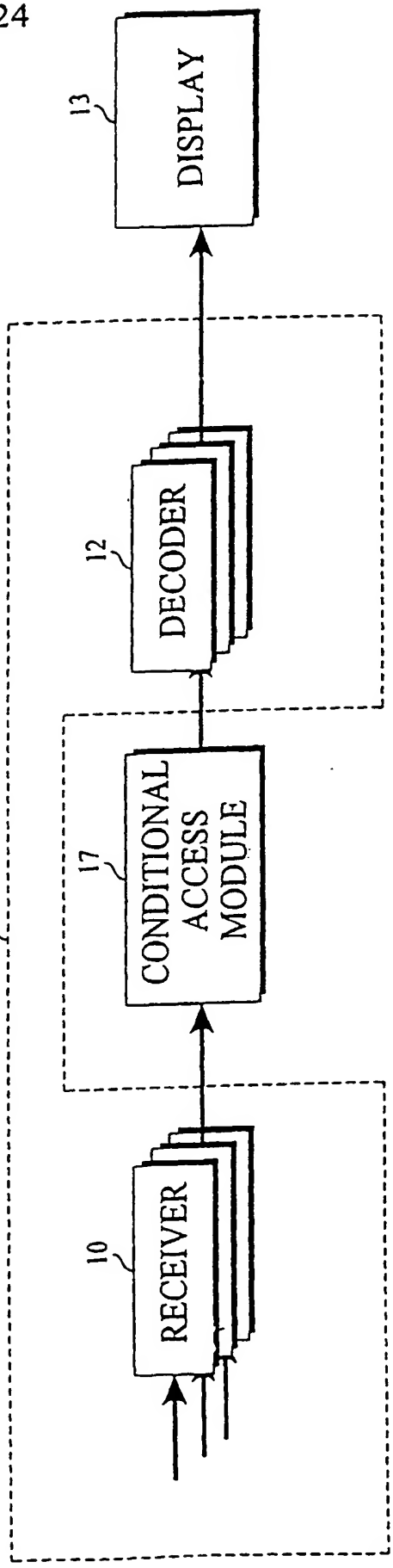

Fig. 2B

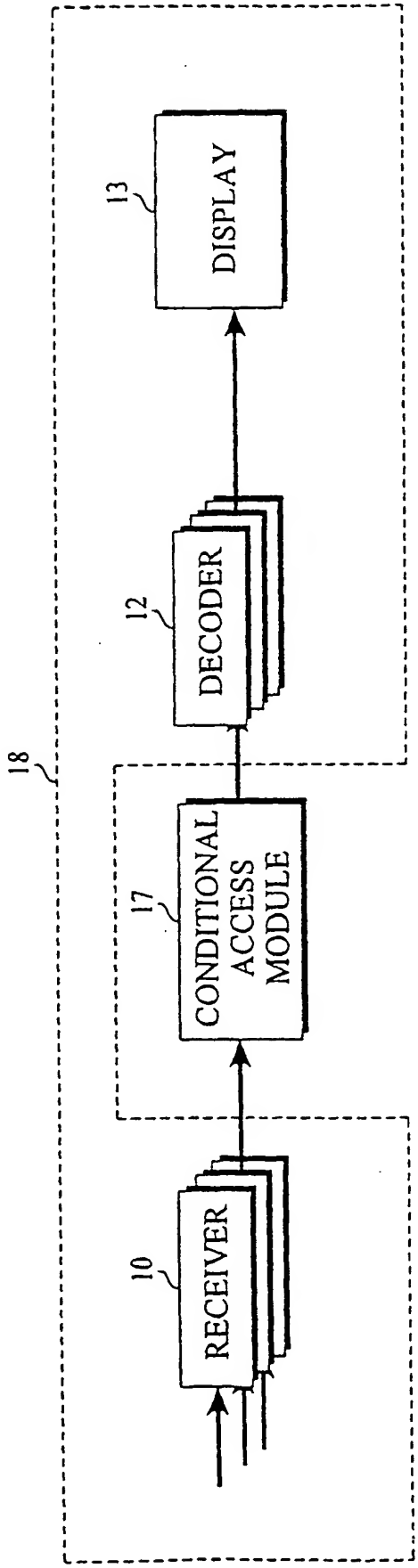
18
13
DISPLAY
12
DECODER
17
CONDITIONAL ACCESS MODULE
10
RECEIVER

Fig. 2C

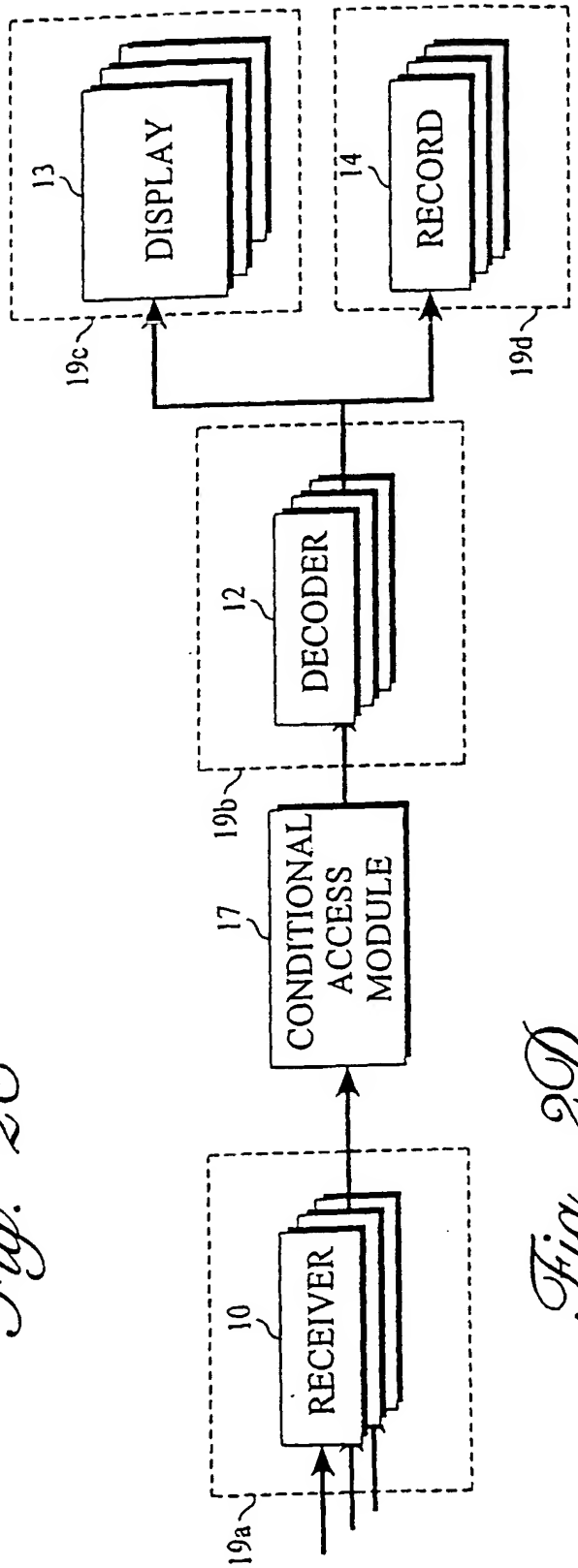
13
DISPLAY
14
RECORD
19c
19d
12
DECODER
19b
17
CONDITIONAL ACCESS MODULE
10
RECEIVER
19a

Fig. 2D

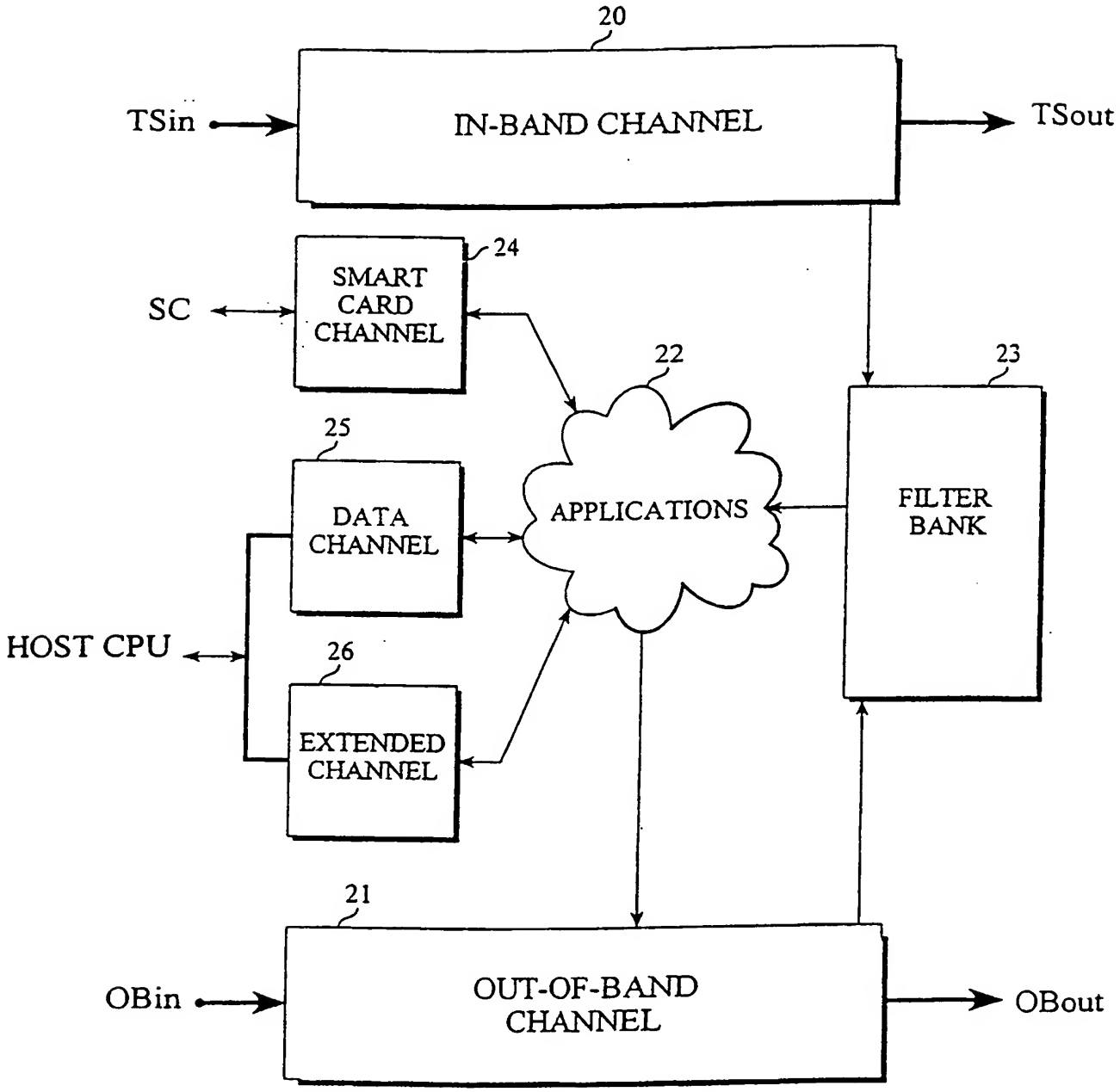

Fig. 3

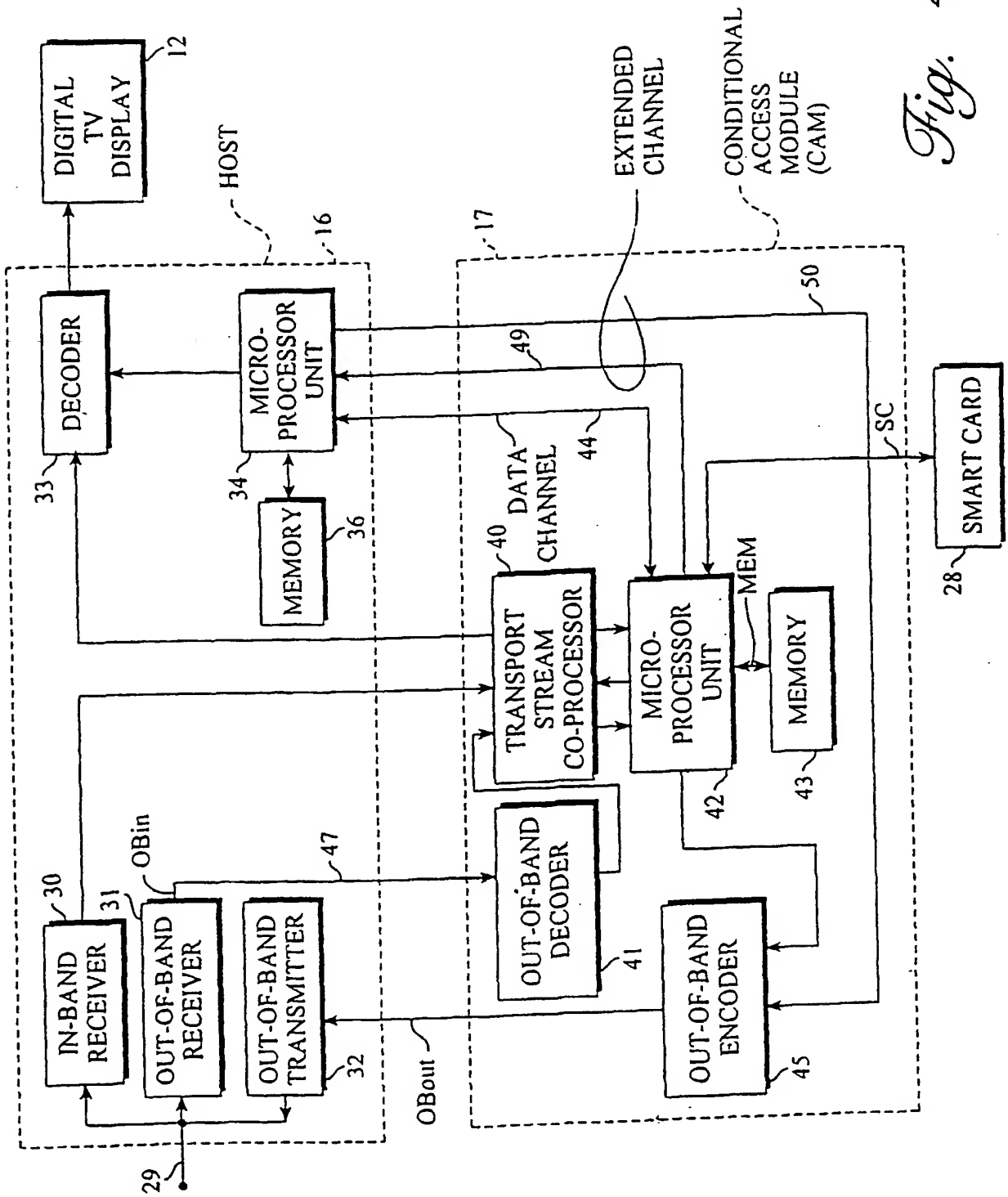

Fig. 4

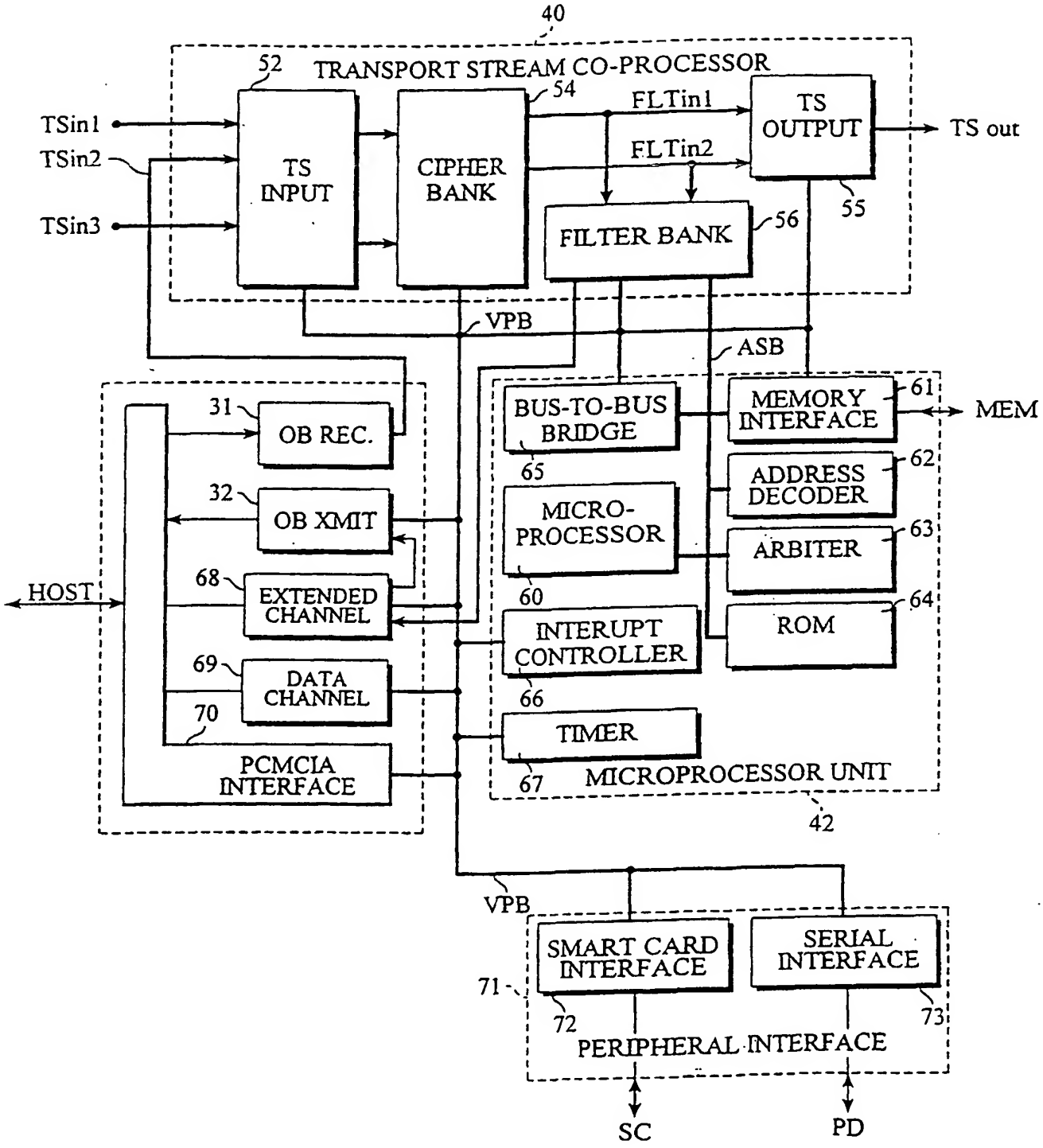

Fig. 5

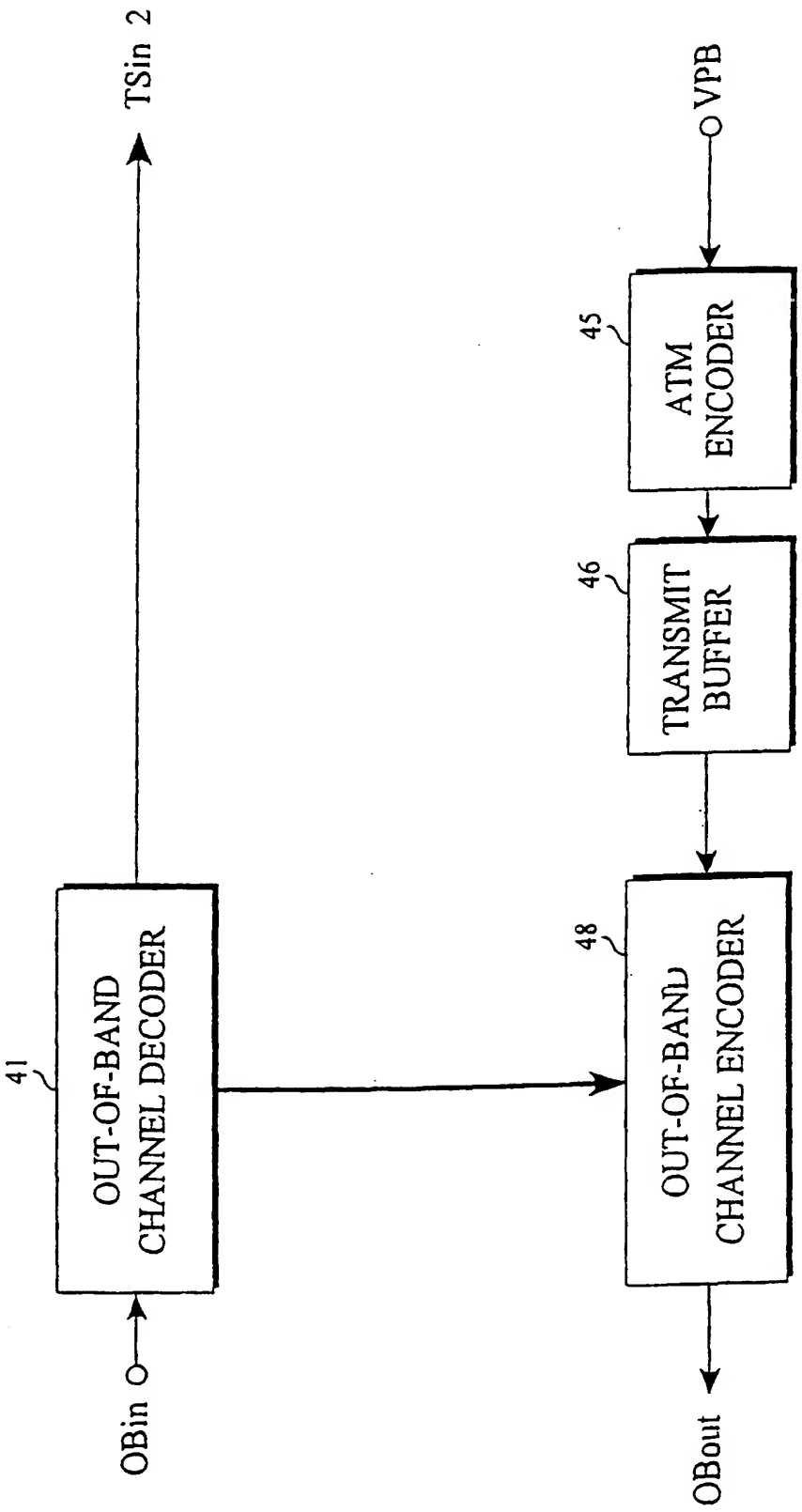

Fig. 6

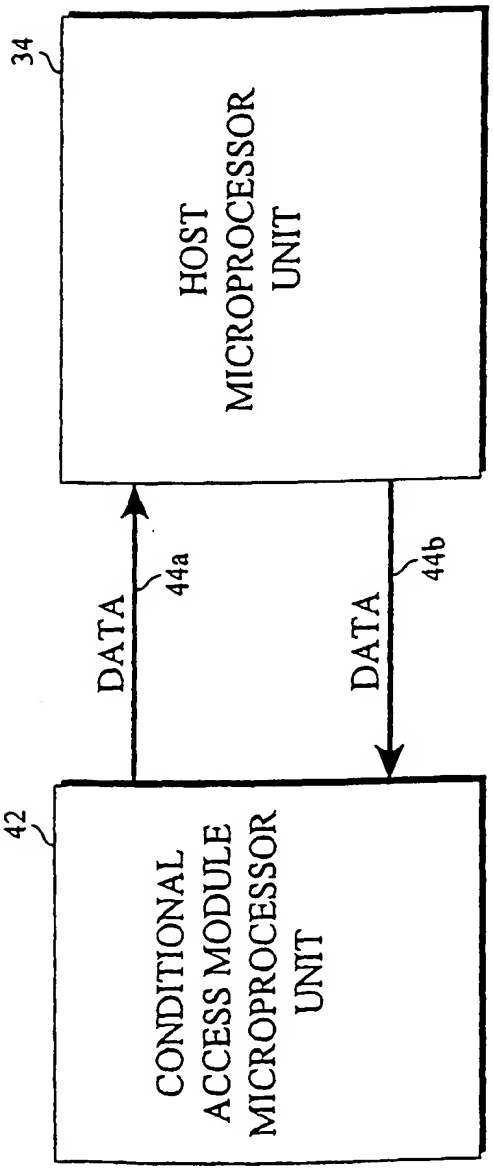

Fig. 7

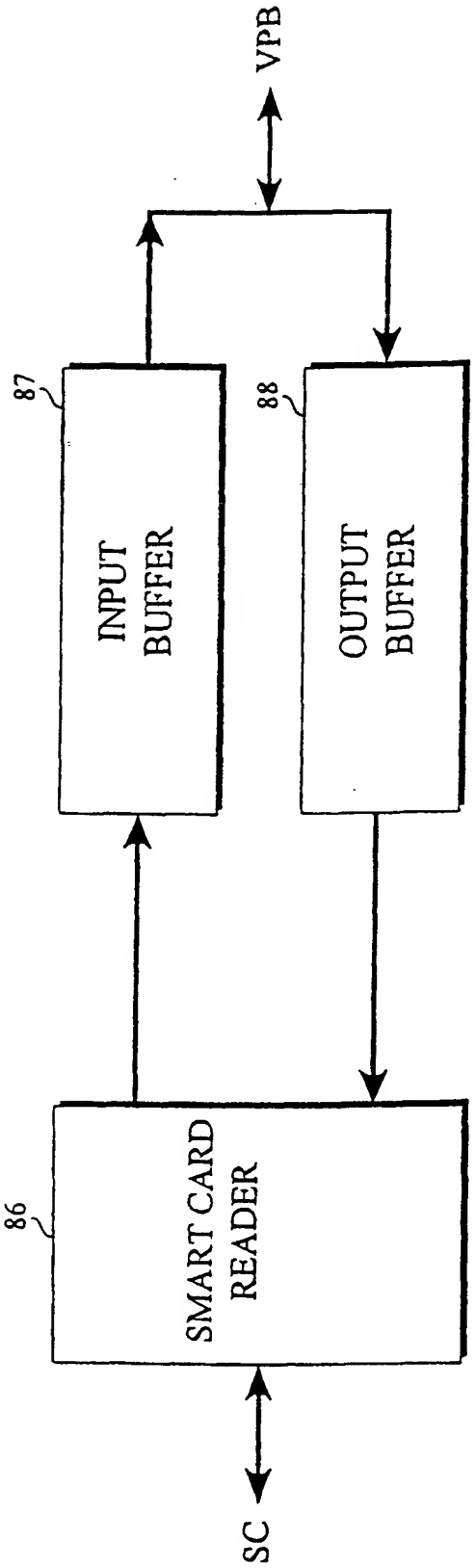

Fig. 8

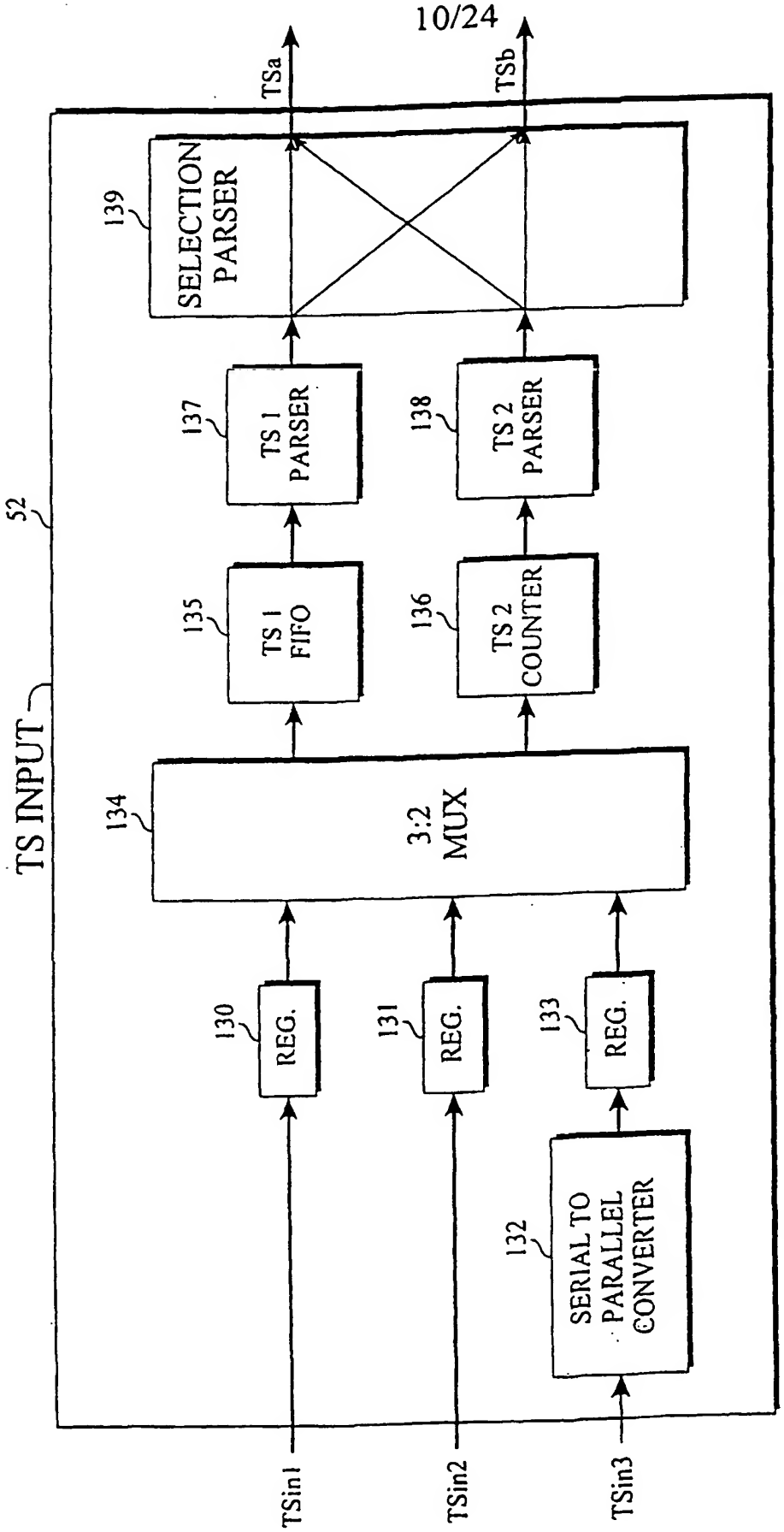

Fig. 9

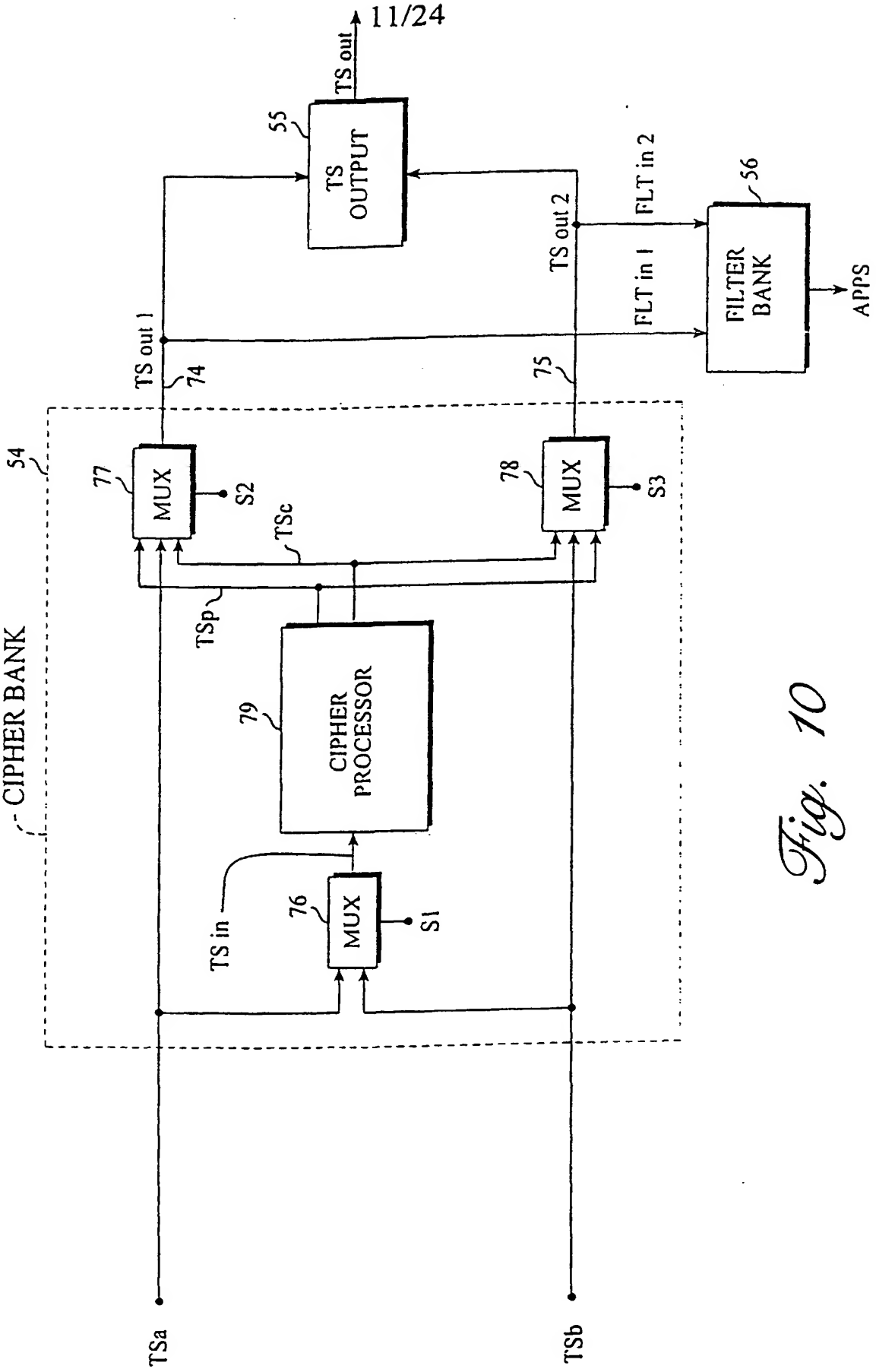
TS out
55
TS OUTPUT
TS out 2
FLT in 2
56
FILTER BANK
APPS
FLT in 1
TS out 1
74
75
54
77
MUX
S2
TSc
78
MUX
S3
CIPHER BANK
TSp
79
CIPHER PROCESSOR
TS in
76
MUX
S1
TSa
TSb

Fig. 10

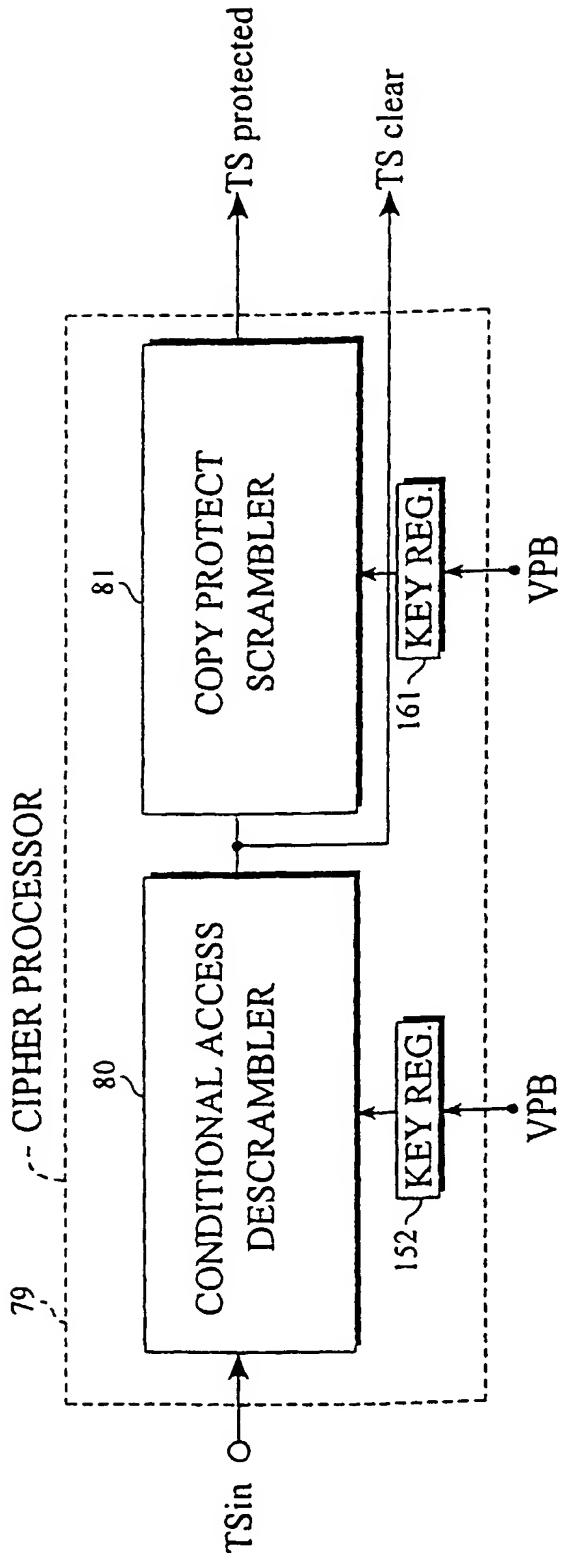

Fig. 11

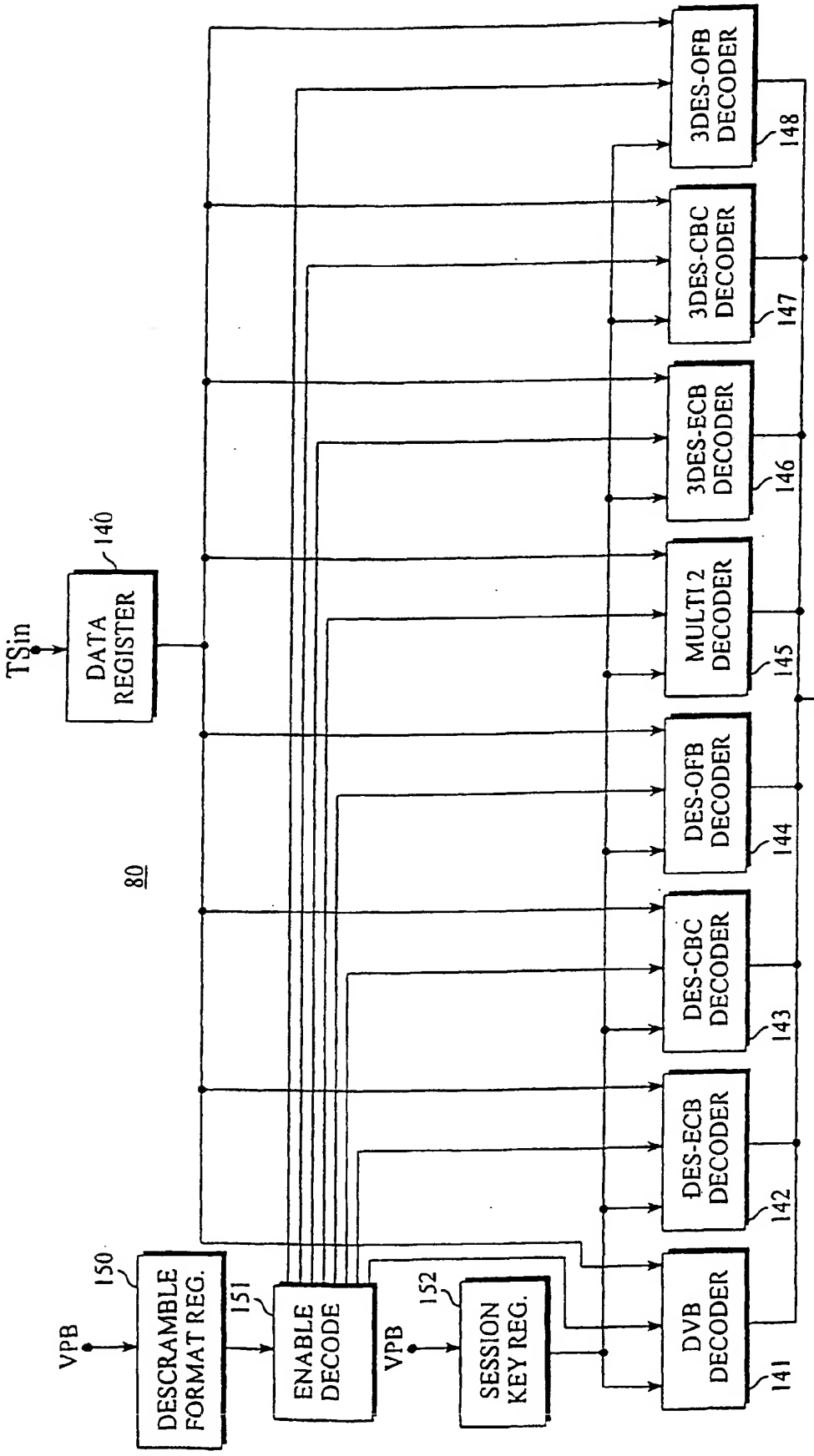

Fig. 12

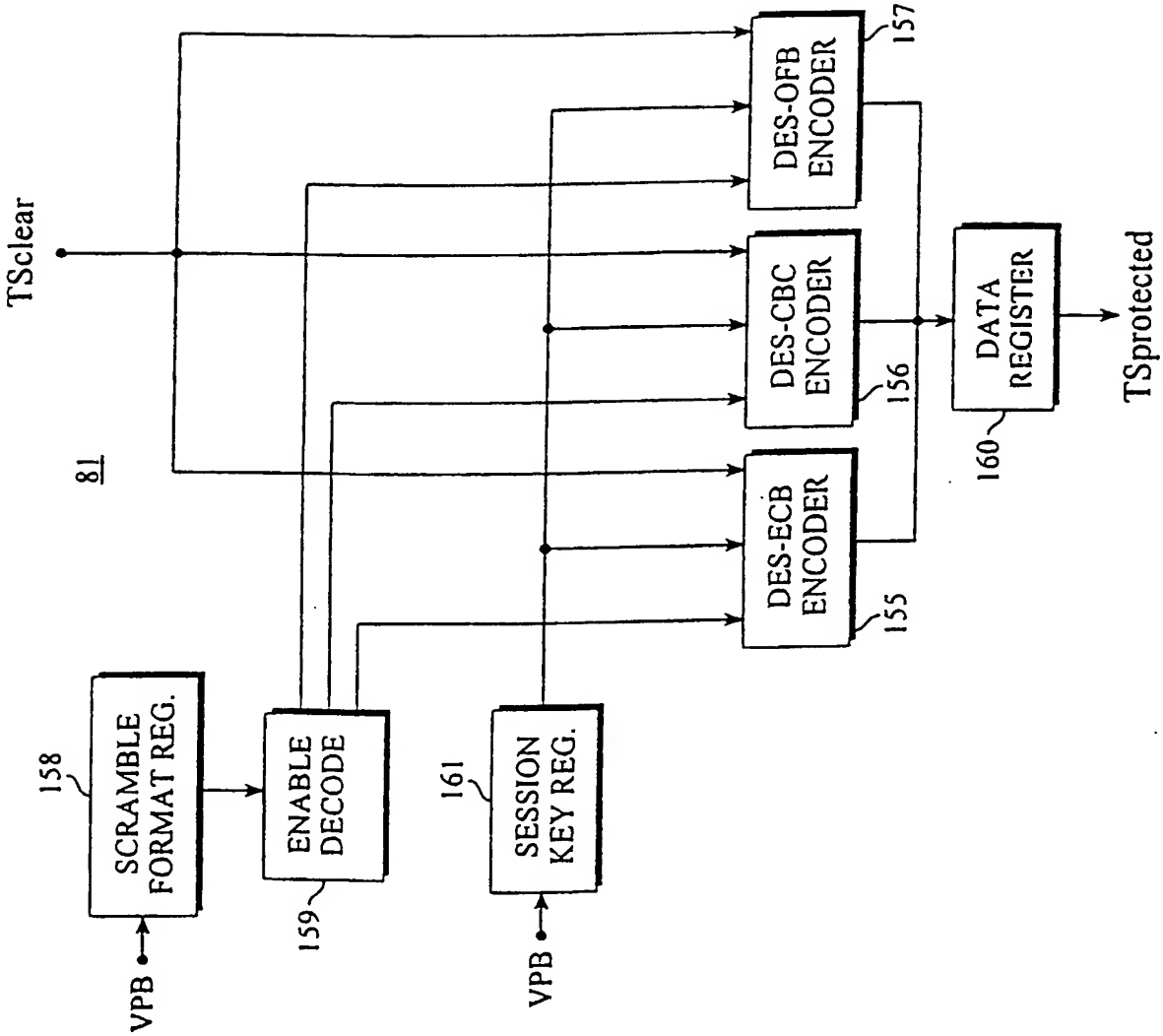

Fig. 13

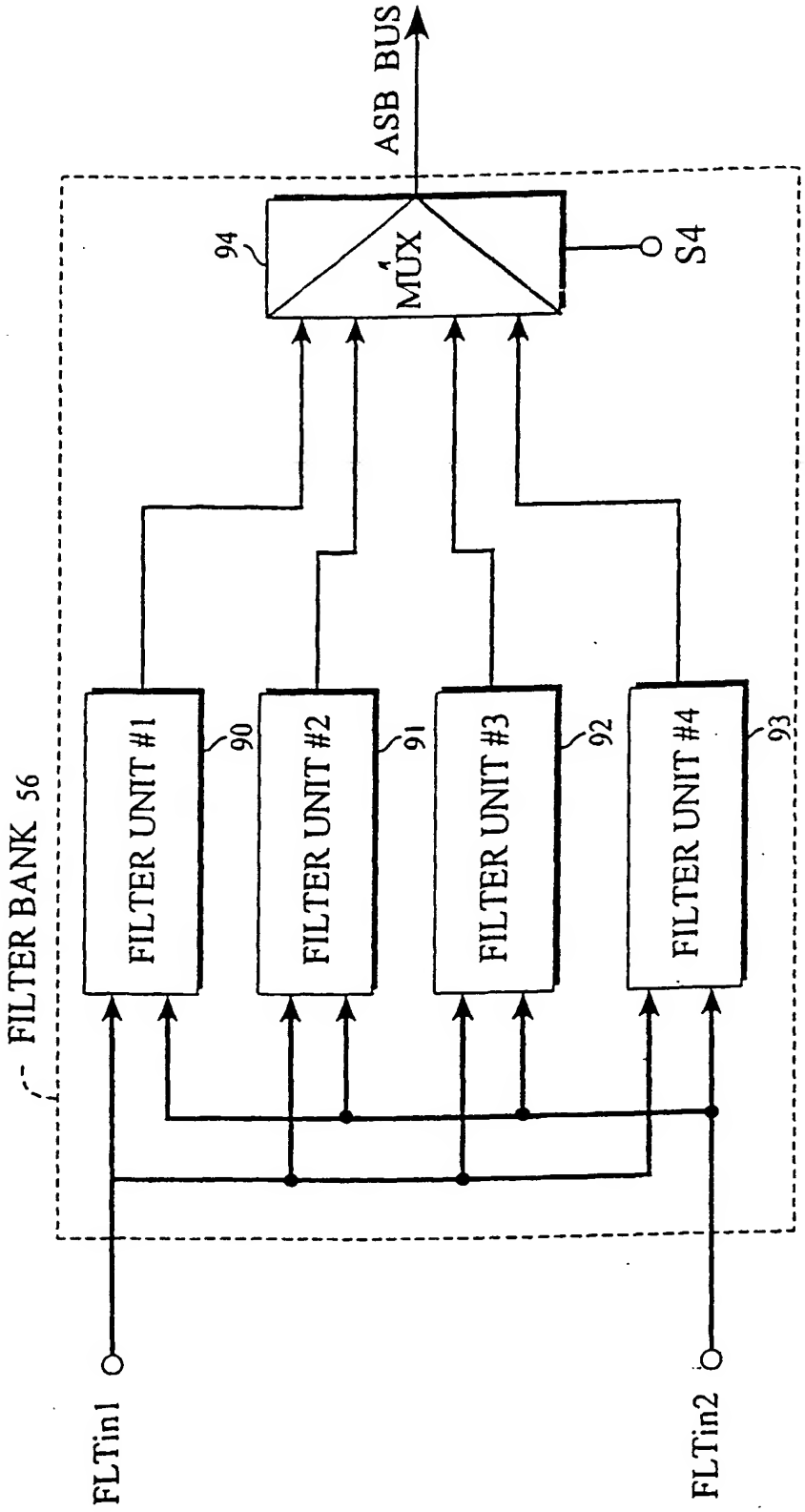

Fig. 14

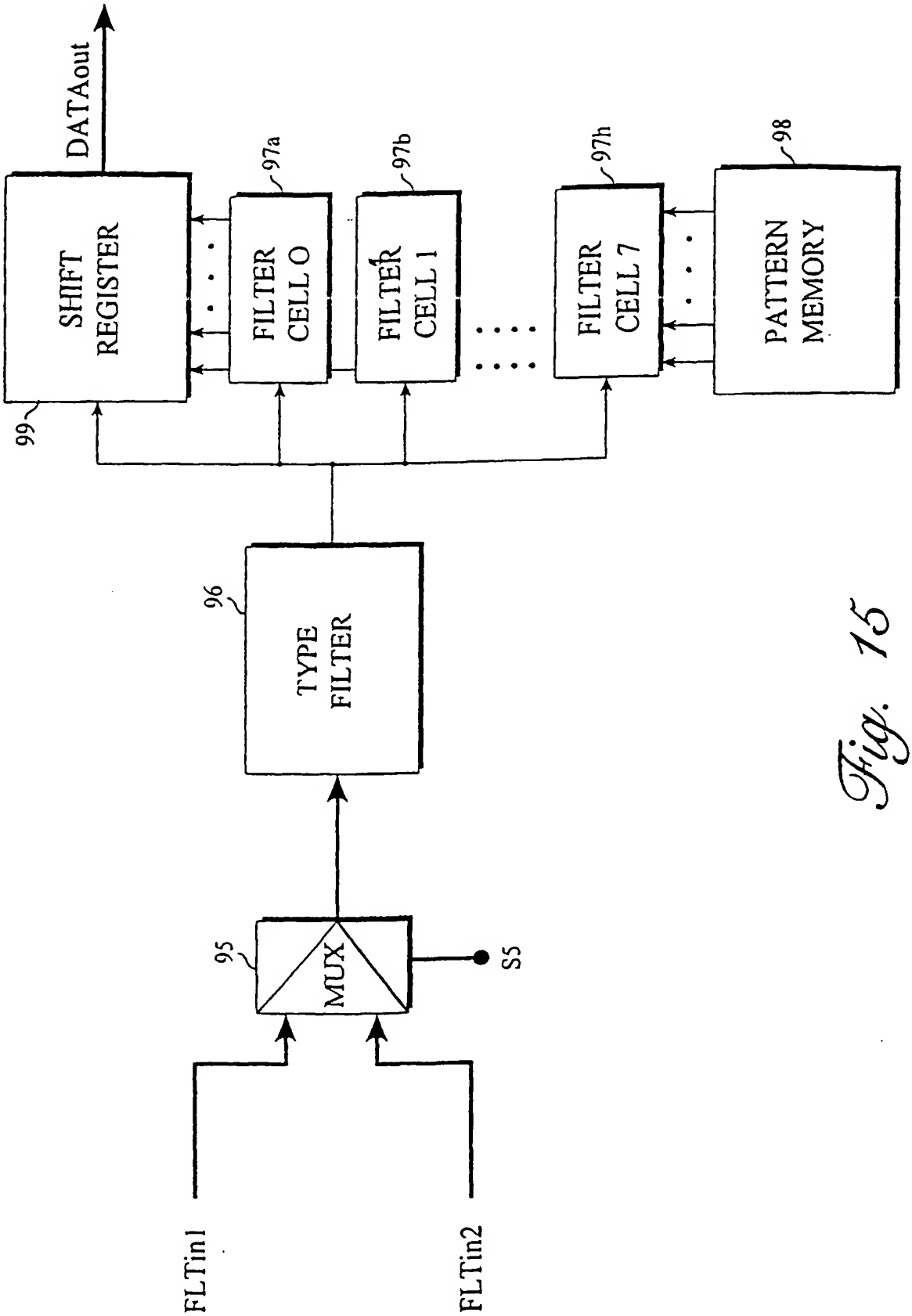
DATAout
SHIFT REGISTER
99
97a
FILTER CELL O
97b
FILTER CELL 1
97h
FILTER CELL 7
98
PATTERN MEMORY
96
TYPE FILTER
95
MUX
S5
FLTin1
FLTin2

Fig. 15

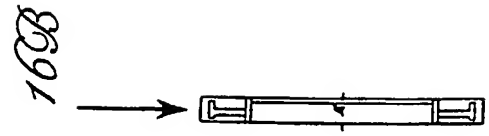

Fig. 16B

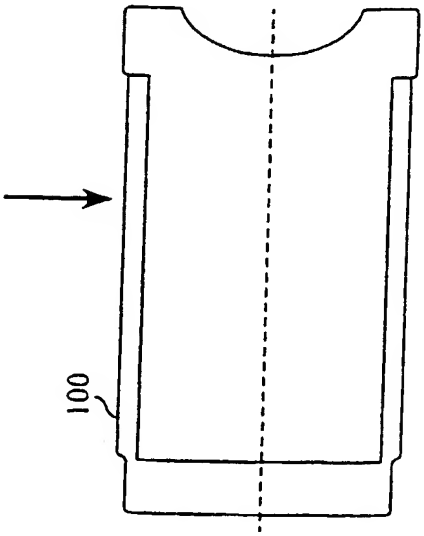

Fig. 16

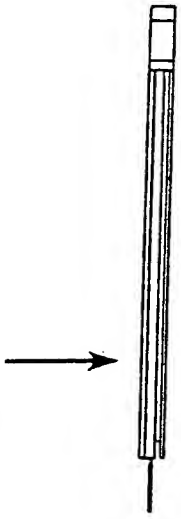

Fig. 16C

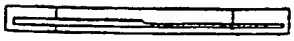

Fig. 16A

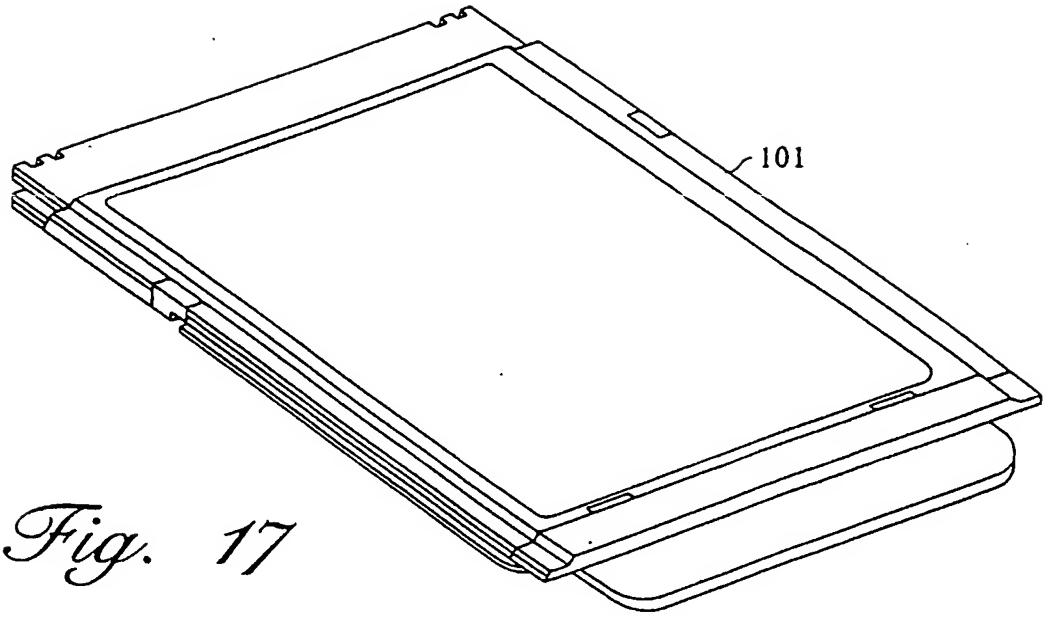

Fig. 17

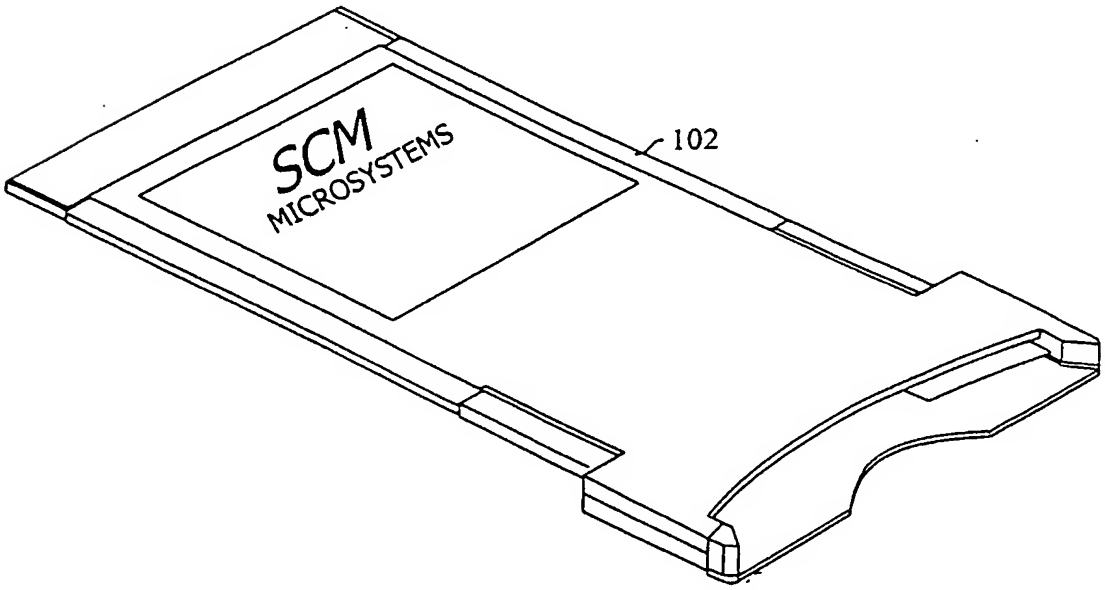

Fig. 18

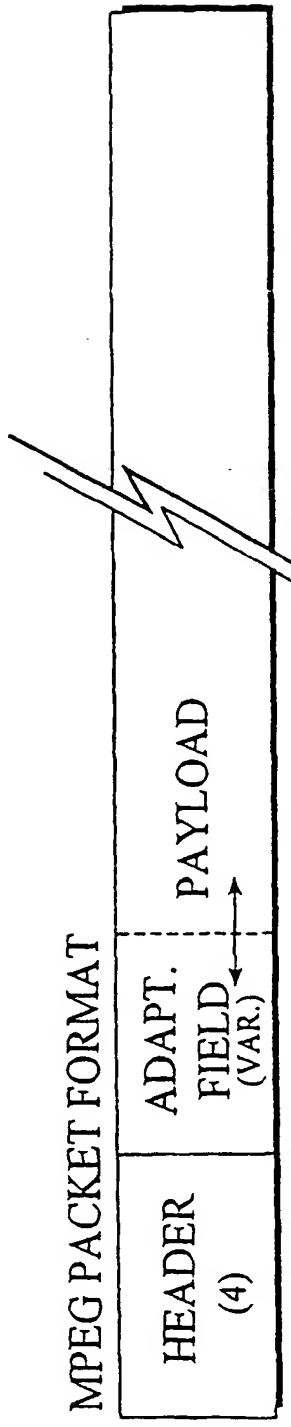

Fig. 19

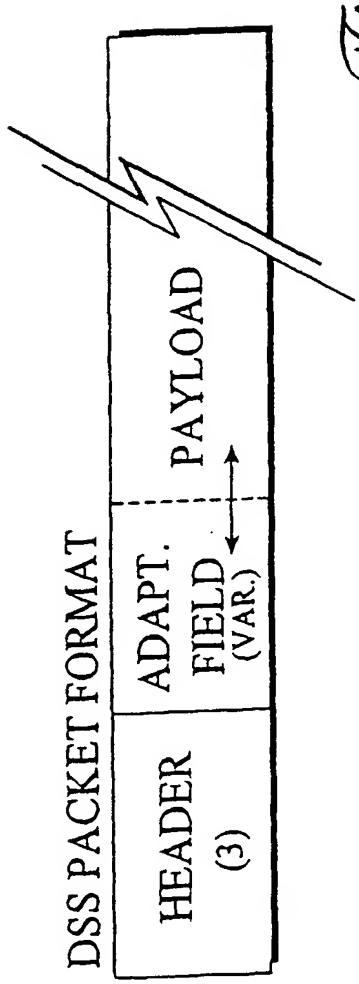

Fig. 20

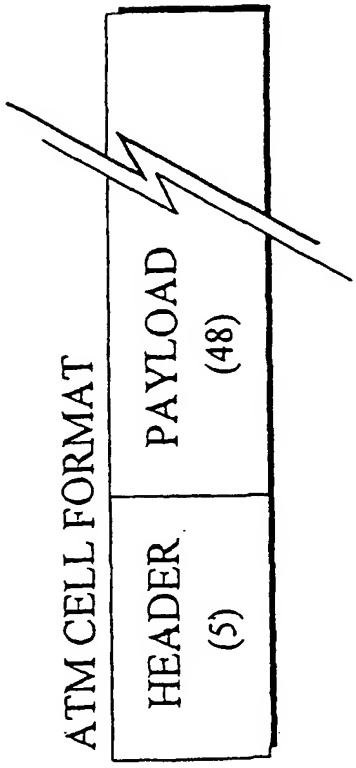

Fig. 21

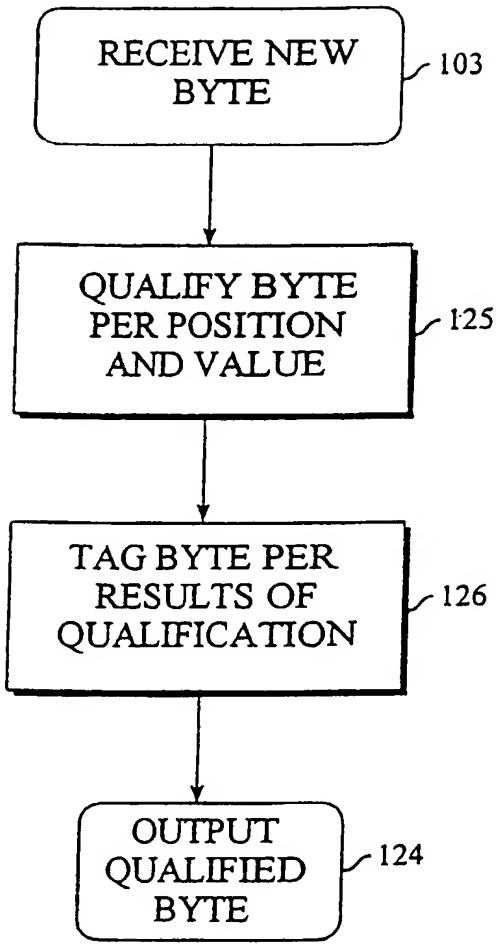
RECEIVE NEW BYTE
103
QUALIFY BYTE PER POSITION AND VALUE
125
TAG BYTE PER RESULTS OF QUALIFICATION
126
OUTPUT QUALIFIED BYTE
124

Fig. 22

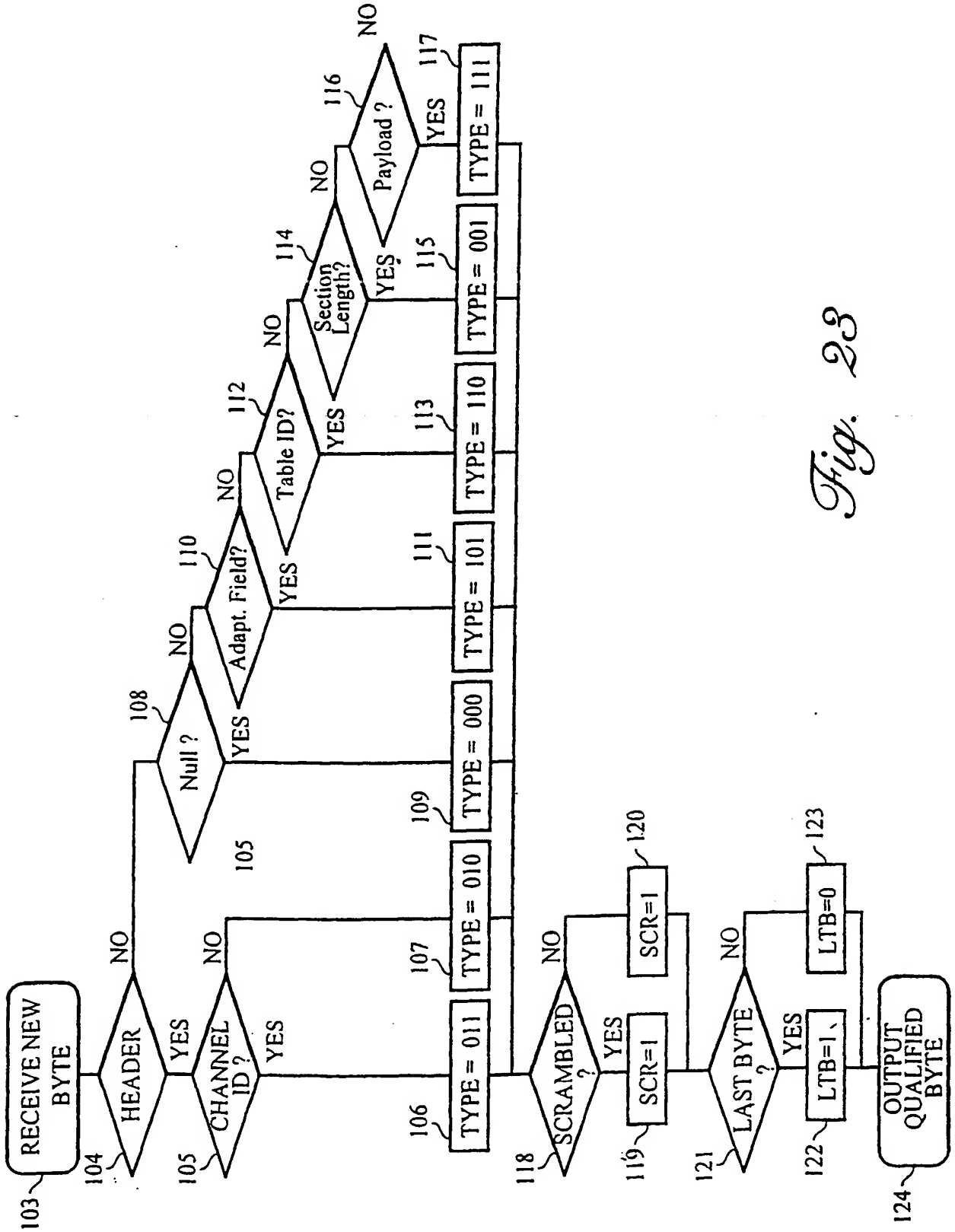

Fig. 23

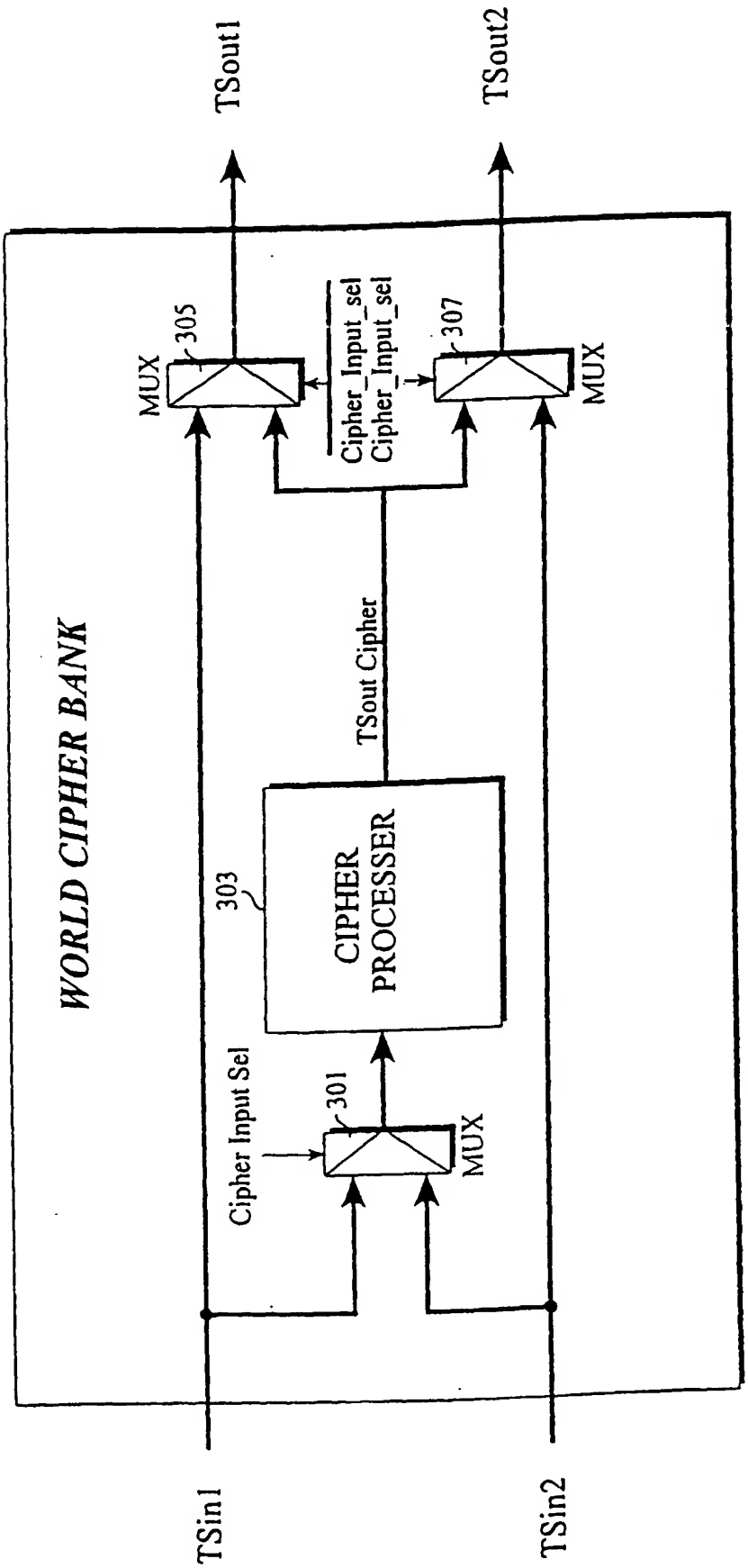
TSout1
TSout2
WORLD CIPHER BANK
MUX
305
Cipher_Input_sel
Cipher_Input_sel
307
MUX
TSout Cipher
303
CIPHER
PROCESSER
Cipher Input Sel
301
MUX
TSin1
TSin2

Fig. 24

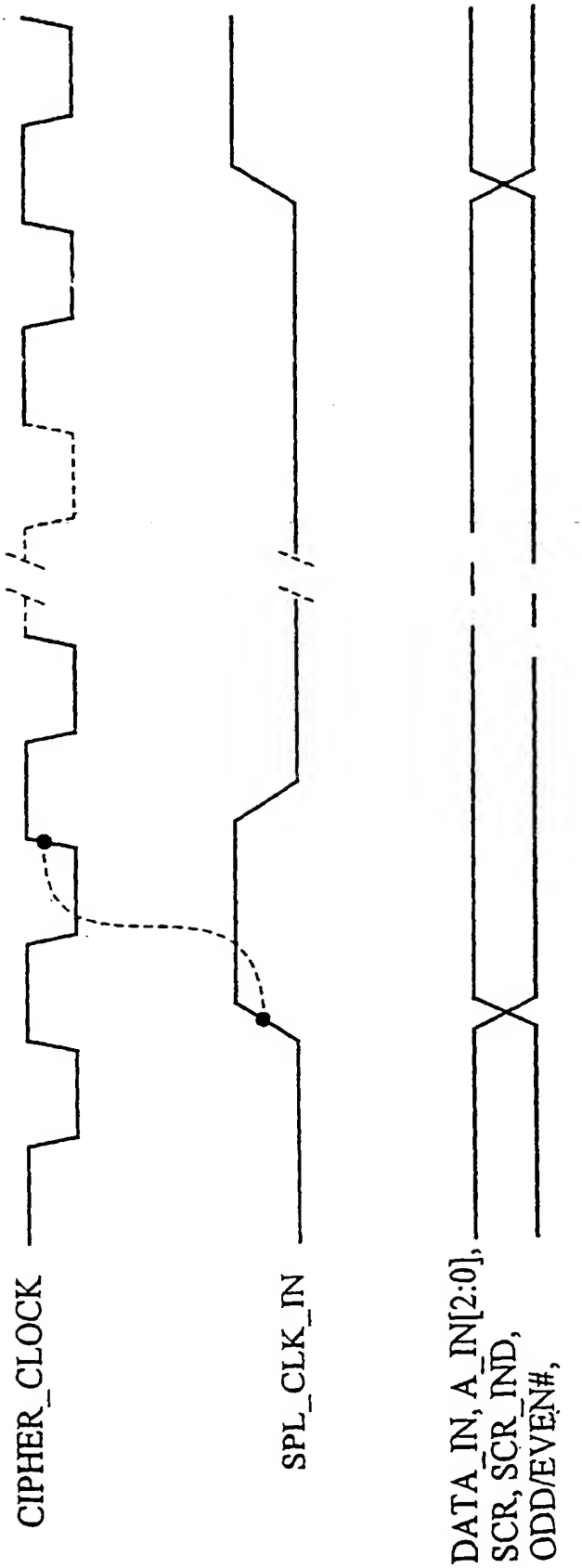

Fig. 25

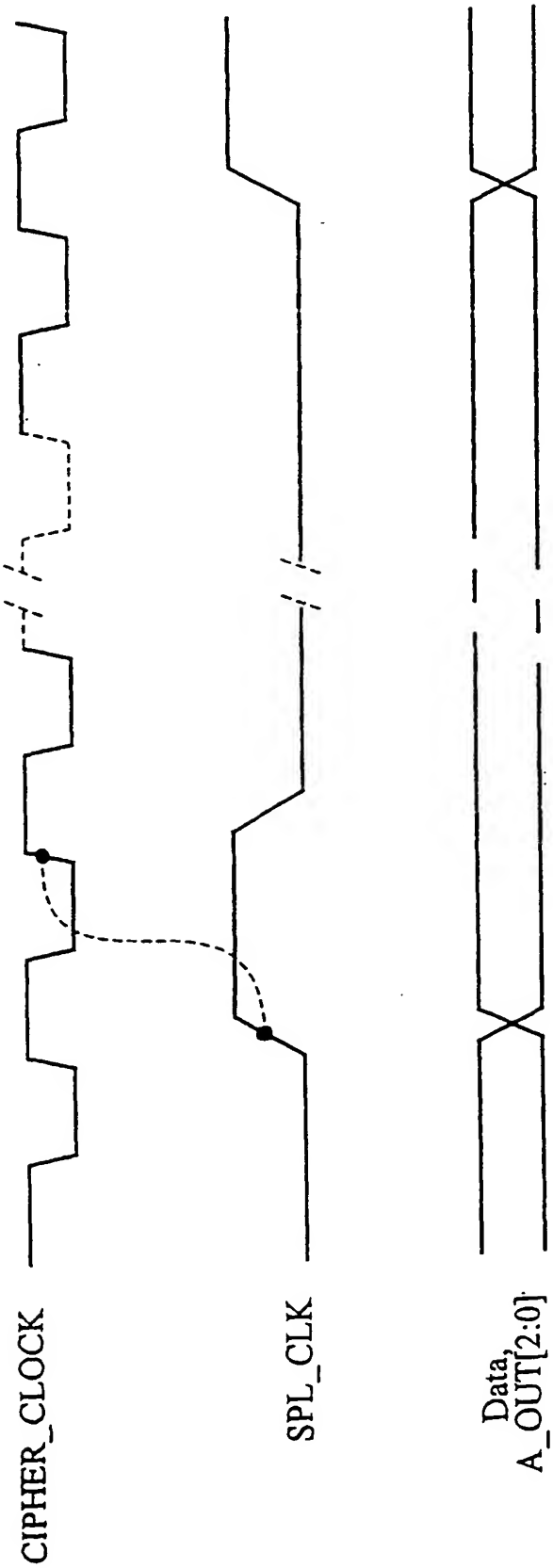

Fig. 26

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
25 May 2001 (25.05.2001)

PCT

(10) International Publication Number
WO 01/37546 A3

(51) International Patent Classification[7]: H04N 5/00, 7/167

(21) International Application Number: PCT/EP00/11483

(22) International Filing Date:
17 November 2000 (17.11.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/444,495 19 November 1999 (19.11.1999) US

(71) Applicant: SCM MICROSYSTEMS GMBH [DE/DE]; Sperl-Ring 4 Hettenshausen, 85276 Pfaffenhofen (DE).

(72) Inventors: VANTALON, Luc; 1396 Cordilleras Avenue, Sunnyvale, CA 94087 (US). CHATAIGNIER, Arnaud; 31, allée de la Granette, F-13600 Ceyreste (FR). GENEVOIS, Christophe; 47, avenue de la Paix, F-13600 La Ciotat (FR).

(74) Agent: DEGWERT, Hartmut; Prinz & Partner, Manzingerweg 7, 81241 München (DE).

(81) Designated States (*national*): JP, SG.

(84) Designated States (*regional*): European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Published:
— *with international search report*

(88) Date of publication of the international search report:
8 November 2001

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 01/37546 A3

(54) Title: DIGITAL TELEVISION METHODS AND APPARATUS

(57) Abstract: Conditional access methods and apparatus are provided for use with digital television receivers and other digital broadband receivers. The methods and apparatus are capable of handling several different digital signal transmission protocols in an automatic and flexible manner. An input unit is provided for analyzing and tagging incoming data bytes so that further processing operations are less dependent on the transmission format being received. A cipher handling unit is provided for adapting in real time the scrambling and descrambling performances to match the requirements of the transmission network and the receiving apparatus. A filtering mechanism is provided for filtering and handling multiple asynchronous data streams in a parallel manner.

INTERNATIONAL SEARCH REPORT

International Application No
PC., EP 00/11483

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04N5/00 H04N7/167

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P,A	WO 00 27114 A (GEN INSTRUMENT CORP ;KASSMAN TODD (US); PETERKA PETR (US); MANGALO) 11 May 2000 (2000-05-11) abstract page 2, line 29 -page 7, line 2 page 8, line 2 -page 12, line 24 ---	1,2, 160-162
A	BUNGUM O W: "TRANSMULTIPLEXING, TRANSCONTROL AND TRANSSCRAMBLING OF MPEG-2/DVB SIGNAL" INTERNATIONAL BROADCASTING CONVENTION, 12 September 1996 (1996-09-12), XP002040478 the whole document --- -/--	1,2, 160-162

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
6 April 2001	11. 06. 01

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Ibruegger, J

4

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PC., EP 00/11483

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 835 493 A (JOHNSON BRIAN ET AL) 10 November 1998 (1998-11-10) abstract column 1, line 28 -column 8, line 10 ---	1,2, 160-162
A	US 5 912 972 A (BARTON JAMES M) 15 June 1999 (1999-06-15) column 1, line 22 -column 4, line 38 ---	1,2, 160-162
P,A	WO 00 54493 A (DIVA SYSTEMS CORP) 14 September 2000 (2000-09-14) page 5, line 15 -page 12, line 20 ---	1,2, 160-162
A	WO 97 18674 A (WYTEC INC) 22 May 1997 (1997-05-22) page 5, line 2-14 page 12, line 18 -page 18, line 19 -----	1,2, 160-162

4

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

national application No.
PCT/EP 00/11483

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☐ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

1,2, 160-162

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. Claims: 1,2,160-162

   Adaptive receiving system for receiving signals in a plurality of transport formats and a plurality of encryption formats, generating transport format independent information, trans-scrambling encrypted portions of the received signals, extracting auxiliary information from the received signals and controlling the trans-scrambling in response to the transport format independent information and the extracted auxiliary information.

2. Claims: 3-7,43-47,72-79

   Reception and qualification of data units, determination of the encryption state, providing a clear output, if the data are unencrypted and performing decryption, if the data are encrypted.

3. Claims: 8-18,39,80-100,130-134

   Handling of a plurality of transport stream formats by a qualification mechanism and a tagging mechanism applying multibit tags to each received data byte.

4. Claims: 19-23,40,41,101-112

   Reception of one or more signals of a selected transport format by a plurality of receivers and selection of a received signal by a security mechanism for removing at least a single security layer.

5. Claims: 24-27

   Reception of one or more signals subject to at least a single predetermined security layer and removal of the at least single security layer.

6. Claims: 28-32

   Selection of a transport stream format and security mechanism for selecting one or more transport streams.

7. Claims: 33-38

   Reception of different digital transmission format data streams, conversion of the data streams into perceivable

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

information via a transmission format independent set of signals.

8. Claim : 42

First testing and tagging, second testing for determining whether data are scrambled and second tagging in response to second testing for assigning a scramble condition tag and transfer of signals for producing usable digital information.

9. Claims: 48-51,52-64

Scrambling/descrambling by pairing of a host with a selected module, selection of a scrambling format and a session key.

10. Claims: 65-69

Scrambler comprising a scramble format register and selection of an encoder by a control signal.

11. Claims: 70,71,126-128

Scrambling by channel change, selection of a descrambling mechanism, changing a session key and loading a new session key.

12. Claims: 113-123

Receiving signals scrambled according to different scrambling formats, descrambling and rescrambling.

13. Claim : 124

Decryption of first type encrypted information and re-encrypting the information with a second type of encryption.

14. Claim : 125

Receiving of qualified information and if the received information is not scrambled passing the information without scrambling.

15. Claim : 129

Pairing of a conditional access module with a selected module, selecting a copy protect mechanism and determining a

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

scrambling session key.

16. Claims: 135,136

Detection of digital patterns within received digital signals and transfer of data bytes associated with the patterns to different end use locations.

17. Claim : 137

Filter for separating a plurality of digital data transport streams intended for different end uses, short and long term storage and multiplexing long and short term stored data in a time shared manner.

18. Claims: 138-157

Scrambling of data in conjunction with recording an descrambling in conjunction with playback.

19. Claim : 158

Multiformat signal system comprising a multitransport receiving system, a multiscrambling system and a multifiltering system.

20. Claim : 159

Use of a tag to determine a descrambling operation and separation of control from content information.

INTERNATIONAL SEARCH REPORT

ormation on patent family members

International Application No
PC., EP 00/11483

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0027114 A	11-05-2000	AU 1455100 A	22-05-2000
US 5835493 A	10-11-1998	US 6002687 A	14-12-1999
US 5912972 A	15-06-1999	US 5646997 A	08-07-1997
		US 6115818 A	05-09-2000
		US 6047374 A	04-04-2000
		US 6101604 A	08-08-2000
		US 6163842 A	19-12-2000
WO 0054493 A	14-09-2000	US 6229895 B	08-05-2001
		AU 3878900 A	28-09-2000
WO 9718674 A	22-05-1997	US 5875396 A	23-02-1999
		CA 2236088 A	22-05-1997
		CN 1202295 A	16-12-1998
		EP 0861559 A	02-09-1998
		JP 2000500628 T	18-01-2000